Security Operations Center

Projektna specifikacija iz predmeta *Bezbednost u sistemima elektronskog poslovanja* i *Sistemi bazirani na znanju.*

Zadatak realizuju timovi od najviše 3 člana. Moguće je polagati samo BSEP deo ili samo SBNZ deo, no sitan dodatni posao će biti neophodan kako bi demonstrirali sve aspekte projekta za predmet koji branite.

Tehnologije koje se koriste za implementaciju bilo koje celine ovog sistema su proizvoljne.

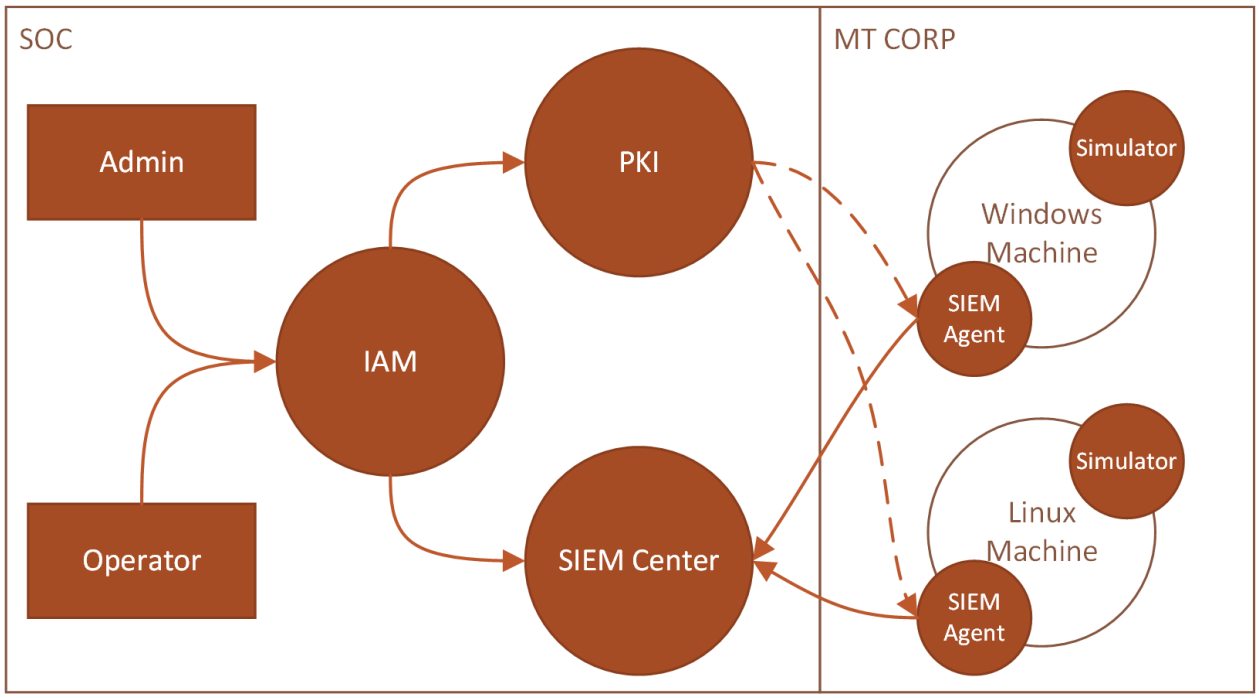
Kontekst

MegaTravel je multinacionalna korporacija koja nudi usluge organizacije putovanja mušterijama širom sveta. Kako bi podržala milione mušterija i hiljade zaposlenih, kao i očuvala položaj svetskog lidera na tržištu, MegaTravel raspolaže sa značajnim brojem softverskih podsistema, od internih alata i informacionih sistema, do servisa dostupnih putem interneta. Zbog velike količine vrednih podataka i svoje pozicije na tržištu, softver ove korporacije predstavlja značajnu metu za napad od strane kriminalaca i konkurenata.

Kako bi obezbedili svoje informacione sisteme i zaštitili se od napadača, MegaTravel poseduje nekoliko centara za bezbednosne operacije (engl. *Security operations center*, u daljem tekstu SOC). SOC predstavlja podsistem koji se sastoji od bezbednosnih alata i osoblja koje upravlja istim, sa ciljem zaštite sistema, detekcijom i pravovremenom reakcijom na napade, kako bi se umanjile negativne posledice istog.

Arhitektura

U ovoj sekciji je izložena arhitektura MegaTravel sistema, sa fokusom na segmentiranju SOC podsistema od ostatka MegaTravel korporativnog sistema (u daljem tekstu MT CORP). Kontekstni dijagram toka podataka projektnog zadatka je prikazan na slici 1.



Slika 1 MegaTravel sistem sa izdvojenim SOC podsistemom

U kontekstu projektnog zadatka, SOC predstavlja skup od tri bezbednosna alata, koji uključuju:

- Alat za podršku infrastrukture javnih ključeva (engl. *Public key infrastructure*, u daljem tekstu *PKI*). Zahtevi za alat, u vidu korisničkih priča, su istaknuti u sekciji 1. PKI.
- Alat za monitoring sistema (engl. *Security information and event management*, u daljem tekstu SIEM). SIEM se sastoji od agenata koji su postavljeni na računare MT CORP sistema i centra koji interaguje sa njima. SIEM je opisan u sekciji 2. SIEM, dok su zahtevi za SIEM centar istaknuti u sekciji 2.1 a za SIEM agenta u sekciji 2.2. Najzad, radi testiranja efektivnosti SIEM alata, neophodno je konstruisati simulatore, čiji zahtevi su istaknuti u sekciji 2.3.
- Alat za centralizovano upravljanje identitetom i pristupom (engl. *Identity and access management*, u daljem tekstu IAM). Zahtevi za alat su istaknuti u sekciji 3. IAM.

1. PKI

Specifikacija projektnog zadatka je definisana kroz niz obimnih korisničkih priča, formiranih od strane admina. Za svaku priču, navedeno je nekoliko teza kako bi se istakli aspekti koji preciznije definišu zadatak i ovo treba uzeti u obzir pored samog teksta korisničke priče. Potrebno je dizajnirati i implementirati PKI vođeni ovim zahtevima.

As a security administrator,
I want to centrally issue certificates for my system's software,
So that I can easily manage the digital identities of software in my system.

- Adminu treba omogućiti da izda bilo koji sertifikat u lancu sertifikata.
- Admin treba da ima uvid u sertifikate koji postoje na sistemu.
- PKI treba da uzme u obzir validnost sertifikata u kontekstu izbora izdavaoca.
- Admin treba što više olakšati popunjavanje svih podataka koji su potrebni za sertifikat.
- Obratiti pažnju na *best practice* konfiguraciju bezbednosnih funkcija koje koristite.

As a security administrator,
I want to revoke certificates when the need arises,
So that I can maintain the integrity of my PKI.

- PKI treba da pruži servis za proveru da li je sertifikat povučen.

As a security administrator,
I want to control which applications can communicate with each other,
So that I can prevent threat agents from harming my system.

- Ako app A može da komunicira sa app B, app B može da komunicira sa app A.
- PKI može, ali ne mora samostalno da rešava ovaj zahtev, no treba što više da podrži admina i da tim ima jasnu sliku kako se rešava deo koji PKI ne rešava.

As a security administrator,
I want to securely distribute digital certificates to the different software,
So that I can efficiently replace and install certificates across the system.

- PKI može, ali ne mora samostalno da rešava ovaj zahtev, no treba što više da podrži admina i da tim ima jasnu sliku kako se rešava deo koji PKI ne rešava.
- Obratite pažnju na zahtev da distribuiranje bude bezbedno i efikasno.
- Na odbrani, tim treba da ima jasnu sliku koji su koraci koje će admin da radi prilikom inicijalne instalacije sertifikata (npr. kada se sistem proširi novim softverom), kao i šta će se dešavati kada je potrebno zameniti istekli sertifikat.

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 SBZ. 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, indeksiranje i skladištenje logova dobavljanih od strane SIEM agenata. Potrebno je istražiti koji indeksi imaju smisla kako bi se efikasnije vršili upiti potrebni za pretragu i alarme;
- Operater i admin mogu da koriste funkcije prikaza i pretraga logova po različitim poljima, sa mogućnošću upotrebe regularnih izraza (omogućiti i pretragu logova u radnoj memoriji rule engina-a);
- Operater i admin mogu da pregledaju alarme;
- Operater može da dodaje nova pravila za alarme i aktivnosti opisane ispod, 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* pri čemu je moguća upotreba logičkih operatora AND, OR i NOT između izraza.
- 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 plaćanje aktiviraju alarm za payment sistem
- Zahtevi koji su povezani sa podsistemom za prijavljivanje korisnika aktiviraju brute-force alarm

  Navedeni alarmi su medjusobno isključivi, aktivira se alarm sa najvećim prioritetom. Prioritet alarma se određuje na osnovu broja zahteva navedenog tipa pomnoženih sa modifikatorom. Modifikatori su sledeći:

  - Za DoS napad modifikator je 1,
  - Za payment napad modifikator je 3,

- Za brute-force napad modifikator je 5.

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 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.

2.2. SIEM agent

SIEM agent predstavlja jednostavnu aplikaciju koja se postavlja na računar čiji logovi žele da se prate. Agent ima konfiguracioni fajl koji sadrži spisak direktorijuma koji sadrže logove koje treba da prati na datoj mašini. Kao minimalan skup log datoteka, agenti moraju biti u stanju da čitaju logove operativnog sistema (Linux i Windows), kao i logove proizvoljnog broja drugih izvora (npr. veb-server, aplikacija).

Pored praćenja upisa novih stavki u posmatrane log datoteke, agent treba da podrži filtrirano prosleđivanje novih upisa ka SIEM centru za svaki izvor koji prati. Filteri su definisani u vidu regularnih izraza u sklopu konfiguracije agenta, gde se šalju samo logovi koji prođu sve filtere.

Najzad, agent treba da podrži *real-time* režim rada i *batch processing* za svaki izvor koji prati, gde je ideja da *real-time* režim šalje stavke kako se upisuju u log, dok je za *batch processing* potrebno definisati vremenski interval nakon čijeg isteka se šalju svi zapisi koji su se stvorili u međuvremenu.

2.3. Simulator

Simulator predstavlja skriptu koja generiše događaje sistema koji se potom beleže u log datoteku. Simulator je *state* mašina, koja treba da podrži nekoliko stanja rada simulirane aplikacije (koja treba da ima smisla za kontekst MegaTravel korporacije). U stanjima normalnog rada, simulator treba da generiše događaje koji su relevantni za alarme definisane u tački 2.1., ali ne treba da okine alarme. U stanjima napada, simulator treba da generiše logove tako da okine neke od alarma iz sekcije 2.1.

Potrebno je definisati više stanja za normalan rad i za napade. Format log-a treba da bude po uzoru na *syslog* format i IEC 62443-4-2 standard.

3. IAM

Potrebno je omogućiti *single sign-on* (u daljem tekstu SSO) prijavu na PKI i SIEM alat. Mehanizam za SSO se može implementirati konfigurisanjem gotovih rešenja, poput Active Directory ili Keycloak i njihovom integracijom sa ostatkom sistema.

4. Bezbednost SOC podsistema

Osetljivi podaci sa kojim aplikacija radi treba da budu obezbeđeni u skladištu, u transportu i tokom upotrebe. Identifikovati osetljive podatke i definisati i implementirati prikladne bezbednosne kontrole. Podaci čije skladištenje se ne može izbeći treba da budu šifrovani ili heširani ukoliko je to prikladno. Logovi koji se razmenjuju treba da budu digitalno potpisani od strane agenta koji ih šalje, i komunikacija treba da bude zaštićena od *reply* napada. Komunikacija između veb-čitača i servera treba da bude zaštićena sigurnom konfiguracijom HTTPS protokola. Sertifikate generisati putem PKI alata.

Korisnički interfejs alata treba da podrži prikladne mehanizme za autentifikaciju i autorizaciju. Registraciju korisnika izvršiti upotrebom SQL skripti. Autorizacija podrazumeva kontrolu pristupa po RBAC modelu.

Kompletan SOC sa svim svojim *endpoint*-ima treba da ima regulisane sve rizike sa OWASP Top 10 liste.