VOJNI MONITORING

BEZBEDNOST U SISTEMIMA ELEKTRONSKOG POSLOVANJA 2019/2020

PROJEKTNA SPECIFIKACIJA

Sadržaj

1. UVOD

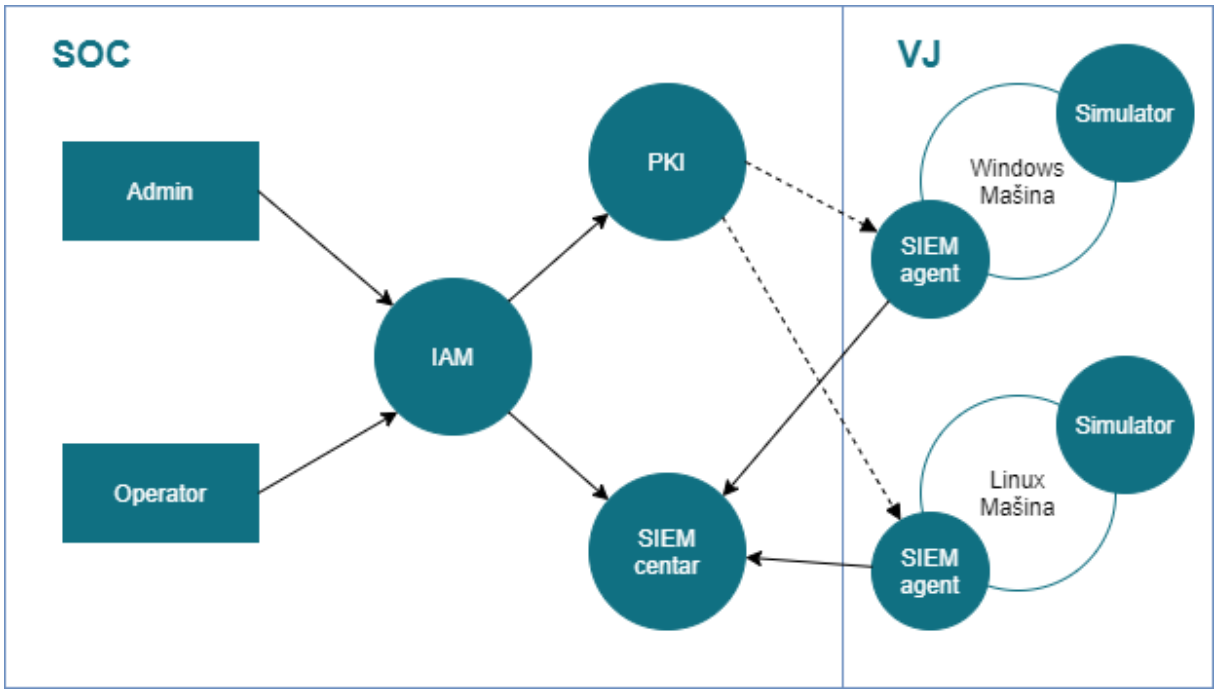
DefenceFirst je multinacionalna korporacija koja pruža podršku u vidu monitoringa vojnim jedinicama. Vojne jedinice brane države od oružanog ugrožavanja spolja i izvršavanja drugih misija i zadataka u skladu sa zakonima i principima međunarodnog prava. One raspolažu sa velikom količinom vrednih i osetljivih podataka koje, u slučaju da dođu u posed nekog drugog lica, mogu da načine veliku štetu. Softver *DefenceFirst*-a predstavlja značajnu metu za napad od strane terorista, kriminalaca i država, čije vojne jedinice ne sarađuju sa ovom korporacijom.

DefenceFirst raspolaže sa velikim brojem softverskih podsistema, od internih alata i informacionih sistema, do servisa dostupnih putem interneta i na taj način se nameće kao lider u ovom domenu. *DefenceFirst* (u daljem tekstu DF) poseduje nekoliko centara za bezbednosne operacije (engl. *Security operations center*, u daljem tekstu SOC), koji obezbeđuju sisteme i štite od napadača. SOC predstavlja sistem koji se sastoji od bezbednosnih alata i osoblja. Cilj je zaštita sistema, detekcija i pravovremenom reakcija na napade, kako bi se umanjile negativne posledice istog.

2. ARHITEKTURA SISTEMA

U ovoj sekciji je izložena arhitektura SOC-a DF sistema i njena povezanost sa vojnim jedinicama (VJ).

Kontekstni dijagram toka podataka projektnog zadatka je prikazan na slici 1.



Slika 1 Kontekstni dijagram toka podataka

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

- **PKI** - Alat za podršku infrastrukture javnih ključeva (engl. *Public key infrastructure*, u daljem tekstu *PKI*). Zahtevi za alat, u vidu korisničkih priča, su istaknuti u poglavlju 3.
- **SIEM** - Alat za monitoring sistema (engl. *Security information and event management*, u daljem tekstu SIEM). SIEM se sastoji od **SIEM agenata** koji su postavljeni na računare vojnih jedinica i **SIEM centra,** koji interaguje sa njima. SIEM je opisan u poglavlju 4.
- **IAM** - (Opciono) Alat za centralizovano upravljanje identitetom i pristupom (engl. *Identity and access management*, u daljem tekstu IAM). Zahtevi za alat su istaknuti u sekciji *6.1 Single sign-on*.

3. ALAT ZA PODRŠKU INFRASTRUKTURE JAVNIH KLJUČEVA

Bitan čvor za bezbednost DF sistema predstavlja podsistem za infrastrukturu javnih ključeva (u daljem tekstu *PKI*). Uz pomoć ovog podsistema, security administrator (u daljem tekstu *admin*) može da poveća bezbednost DF sistema, tako što:

- Omogućuje autentifikaciju softverskih sistema;
- Pruža podršku za kontrolu pristupa između softverskih sistema;
- Štiti poverljivost i integritet poruka koje se razmenjuju između softvera i ljudi, putem šifrovane komunikacije.

Potrebno je dizajnirati i implementirati PKI vođen sledećim zahtevima:

- Admin može centralizovano da izdaje sertifikate za digitalne entitete u svom sistemu.
    a. Adminu treba omogućiti da izda bilo koji sertifikat u lancu sertifikata.
    b. Admin treba da ima uvid u sertifikate koji postoje na sistemu.
    c. PKI treba da uzme u obzir validnost sertifikata u kontekstu izbora izdavaoca.
    d. Potrebno je omogućiti templejte za sertifikate, gde se templejtom definišu ekstenzije koje će ući u sertifikat, a pre svega namena sertifikata.
    e. Adminu treba što više olakšati popunjavanje podataka koji su potrebni za sertifikat.
    f. Obratiti pažnju na best practice konfiguraciju bezbednosnih funkcija koje koristite.
    g. Obratite pažnju na vreme trajanja sertifikata (root CA, subordinate/intermediate CA, end user). Isto tako razmislite o “trajanju” privatnog ključa CA, tj. do kada se može koristiti za potpisivanje sertifikata.
- Admin ima mogućnost da povuče sertifikat.
    a. PKI treba da pruži servis za proveru da li je sertifikat povučen.
- Admin može efikasno da distribuira sertifikate, tj. da ih inicijalno instalira, kada se sistem proširim novim softverom, ili da zameni istekli sertifikat.
    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.
    b. Obratite pažnju na zahtev da distribuiranje bude bezbedno i efikasno.
    c. 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.

4. SIEM PODSISTEM

SIEM predstavlja softver koji prikuplja, normalizuje, filtrira i korelira događaje, kako bi detektovao, alarmirao i reagovao na potencijalne napade i bezbednosne probleme. On se koristi za monitoring informacionih sistema vojnih jedinica. 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 (npr. potrebno je detektovati i izvršiti alarmiranje kada je sto puta u roku od 60 sekundi pokušana prijava na sistem sa istim korisničkim imenom).

SIEM podsistem se sastoji od dve različite aplikacije, SIEM agenta i SIEM centra.

4.1 SIEM agent

SIEM agent predstavlja jednostavnu aplikaciju koja se postavlja na računar čiji logovi treba da se prate. Log zapisi koje generišu aplikacije i operativni sistemi nekog postrojenja su veoma korisni, kako sa aspekta debagovanja problema, tako i za potrebe bezbednosti. Log zapisi predstavljaju osnovni mehanizam za postizanje neporecivosti. Dodatno, kolekcije log zapisa se mogu slati alatima za *monitoring*, poput SIEM alata, čiji zadatak je da prati događaje u sistemu i da okine alarm svaki put kada se sumnjivo ponašanje detektuje.

SIEM agent treba da podrži sledeće funkcionalnosti:

- Parsiranje zapisa u standardizovan format (može da se izbori i sa nestandardnim zapisima).
- Dopunjavanje log zapisa sa informacijama koje agent zna, a nedostaju u zapisu.

  Agenti moraju biti u stanju da čitaju logove operativnog sistema (Linux i Windows), kao i logove proizvoljnog broja drugih izvora (npr. veb-server, aplikacija).
- Čitanje zapisa iz definisanih izvora, uključujući foldere, konkretne datoteke i logove operativnog sistema (Windows, Linux).

  Agent ima konfiguracioni fajl koji sadrži spisak direktorijuma koji sadrže logove, koje treba da prati na datoj mašini.
- Za svaki izvor:
  a. Filtriranje zapisa spram liste regexa.

     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
  b. Period čitanja definiše kao batch (u nekom intervalu) ili real-time (svaki put kad se izmeni zapis).

     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.

4.2 SIEM centar (prikupljanje i skladištenje logova)

SIEM centar predstavlja aplikaciju koja vrši obradu logova koje prihvata od agenata. Putem veb-interfejsa, operater i administrator 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;
- Prikaz i pretraga logova po različitim poljima, sa mogućnošću upotrebe regularnih izraza;
- Pregled alarma i kreiranje pravila za okidanje alarma;
- Generisanje izveštaja bitnih aktivnosti u određenom vremenskom periodu od strane operatera i administatora (broj logova po sistemu, broj logova po mašinama, broj alarma po sistemu, broj alarma po mašini, itd.).

4.2.1 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. Mali podskup ovih događaja 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 ili na nivou simuliranog informacionog sistema;
- Pojava log-a čiji tip je ERROR.

4.3 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 vojnih jedinica). Jedan skup stanja simulira normalan rad aplikacije, a drugi skup aplikaciju pod napadom. U stanjima normalnog rada, simulator treba da generiše događaje koji su relevantni za kreirane alarme, ali ne treba da ih okine. U stanjima napada, simulator treba da generiše logove tako da okine neke od kreiranih alarma.

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

5. NEFUNKCIONALNI ZAHTEVI

5.1 Tehnologije

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

Obavezno je korišćenje Sistema za kontrolu verzija git. Kao udaljeni repoziorijum, može se koristiti *Github* ili *Gitlab*. Neophodno je da projekat bude u privatnom repozitorijumu, na koji će predmetni asistent biti dodat kao collaborator/reporter.

Logovi treba da se čuvaju u noSQL bazi, Komponenta za alarmiranje treba da bude bazirana na ECA (Event Condition Action) pravilima, tj. da se za implementaciju koristi Rule-based sistem.

5.2 Bezbednost resursa

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.

5.3 Upravljanje korisnicima

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, gde postoji rola operatera, koji može da posmatra alarme i pretražuje logove, kao i rola administratora, koji može da kreira pravila alarma, pregleda okinute alarme i pretražuje logove.

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

6. ZADACI ZA OCENU 10

Za najvišu ocenu je neophodno realizovati jednu od celina definisanih u ovom poglavlju.

6.1 Single sign-on

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. Kroz ovaj zadatak, studenti će naučiti kako funkcioniše upravljanje identitetima i pristupom u *enterprise* sistemima sa mnoštvom aplikacija i servisa.

6.2 Secure deployment and disposal

Potrebno je izučiti system hardening i secure disposal procedure i najbolje prakse, i definisati protokol kako će se SecurityFirst postaviti u produkciju i kako će se bezbedno ukloniti kada dođe end-of-life sistema. Kroz ovaj zadatak, studenti će naučiti šta podrazumeva postavka sistema u produkciju, kako se obezbeđuje infrastruktura (hardware, OS, serveri) na koje softver leže, i o čemu sve treba voditi računa kada se softver vadi iz produkcije.

6.3 Penetration testing

Sprovesti penetraciono testiranje veb-aplikacija i servera upotrebom bar dva alata iz grupe: Nmap, Nikto, dirbuster, sqlmap, OWASP ZAP, Burp Suite. Formirati izveštaje penetracionog testa i regulisati ranjivosti. Kroz ovaj zadatak, studenti će naučiti osnove „hakovanja“, odnosno specijalizovanog testiranja uz pomoć alata, čija svrha je identifikacija ranjivosti u softverskom sistemu.

6.4 Performance testing

Potrebno je sistem ostaviti da radi u intenzivnom režimu "preko noći", odnosno duži vremenski period (od 8 do 24 sata). Kada se završi period koji ste odredili potrebno je da izvršite što bolju analizu posledica koje je SIEM sistem imao na rad vaših računara. Koja količina logova je formirana, koje je bilo memorijsko zauzeće. Najzad, sa punim SIEM centrom izvršite analizu performansi vaših upita i alarma i uporedite koji su odzivi u pitanju u odnosu na centar koji ima par stotina logova.

Iskoristite priliku kada napravite distribuiran sistem, koji radi sa velikom količinom podataka, da uradite što više eksperimenata nad njim i što više znanja izvučete. *Google* vam je zgodan resurs za pretragu metrika i mehanizama za ocenjivanje performansi. Ove mehanizme je neophodno ugraditi u softver pre nego što se pokrene eksperiment.

Kompleksnost vašeg eksperimenta, kao i zaključci i znanje koje ste izvukli iz njega je ono što treba na odbrani da prikažete. Timovi treba da formiraju izveštaj svog eksperimenta, uz potrebne vizualizacije (npr. grafove) kojim će pokazati bitne detalje.