Uticaj ljudskog faktora u implementaciji SIEM sistema

Bojana Vilendečić
Direkcija za tehniku
M:tel a.d. Banja Luka
Banja Luka, Bosna i Hercegovina
bojana.vilendecic@gmail.com

Ratko Dejanović
Elektrotehnički fakultet
Univerzitet u Banjoj Luci
Banja Luka, Bosna i Hercegovina
ratko@etfbl.net

Predrag Ćurić
NLB Razvojna banka
Filijala Banja Luka
Banja Luka, Bosna i Hercegovina
predrag.curic@yahoo.com

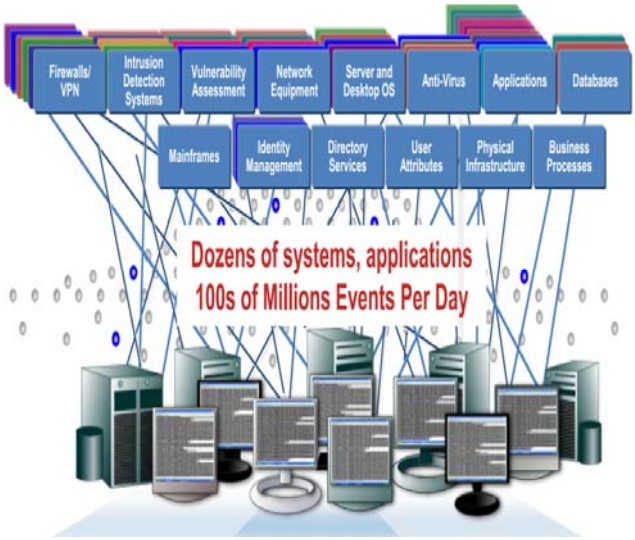
Sadržaj— **U ovom radu je opisan postupak implementacije Security Information and Event Management (SIEM) sistema u IT okruženju i uticaj ljudskog faktora na taj postupak. U uvodnom dijelu su pobrojani sigurnosni sistemi koji se najčešće koriste u korporativnim okruženjima, ključne funkcionalnosti SIEM sistema i njegov značaj u cjelokupnoj sigurnosti IT okruženja. Zatim su navedene preporuke za uspješnu implementaciju SIEM sistema koja ima za cilj viši nivo sigurnosti korporativnog mrežnog okruženja. Dalje je predstavljena optimizacija implementacije SIEM sistema kroz sve faze. Zatim je opisan uticaj ljudskog faktora na implementaciju ovih sistema kao i ljudskih opažanja u korelacijama na detekciju napada.**

Ključne riječi 1; SIEM 2; sigurnost

I. UVOD

U IT okruženju svaki administrator konstantno nadgleda sigurnosne informacije i logove (zapise) koji se generišu na sistemu ne samo radi detekcije grešaka u funkcionisanju već i zbog detekcije napada. Administratori osim pregledanja navedenih zapisa imaju i redovne zadatke koje svakodnevno obavljaju te analiza velikog broja zapisa može predstavljati mukotrpan posao ili se smatrati usputnom obavezom. Oba pristupa imaju negativne posljedice gledano sa sigurnosnog stanovišta. Incidenti se najčešće detektuju analizom logova na više sistema korporativne mreže koje nerijetko administriraju različiti administratori te napad može proći neopaženo bez obzira na vrijeme koje administrator provodi analizirajući zapise jednog sistema. Isto se dešava i kada se zapostavi analiza zapisa i administrator posveti ostalim aktivnostima održavanja sistema.

Uporedo sa trendom povećanja broja sigurnosnih prijetnji i kompleksnosti napada povećava se broj različitih tipova sigurnosnih mehanizama zaštite od napada i monitoringa. Potpuno sigurno okruženje ne postoji. Kompanije koje drže do sigurnosti svog korporativnog okruženja koriste veliki broj sistema zaštite: *Firewall*, sistem za sprečavanje upada – *Intrusion Prevention System*, sistem za zaštitu aplikacija – *Web Application Firewall*, sistem za zaštitu baza podataka – *Database Firewall*, sistem za detekciju upada – *Intrusion Detection System*, sistem za detekciju anomalija – *Anomaly Detection System*, skeneri za testiranje ranjivosti baza podataka i aplikacija, sistem antivirusne zaštite i mnogi drugi. Pobrojani su samo najčešće korišteni sistemi zaštite u korporativnim mrežnim okruženjima što je prikazano na Sl. 1. Dakle, svaki



Slika 1. Mnoštvo sistema i aplikacija korporativne mreže i stotine miliona dnevnih event-a [1]

sistem generiše veliki broj informacija koje mogu biti od krucijalne važnosti za sigurnosti cjelokupnog korporativnog IT okruženja (serveri, radne stanice, sistemi zaštite, sistemi monitoring i mnogi drugi). Dolazi se do zaključka da gotovo svaka kompanija koja ima cilj postaviti nivo sigurnosti na prihvatljiv nivo treba implementirati sistem koji će vršiti centralizovano prikupljanje sigurnosnih informacija i dnevnika događaja, normalizaciju obzirom da svaki sistem generiše specifičan format zapisa, analizu i korelaciju prikupljanih podataka radi detekcije sigurnosnih napada i automatizacije svega navedenog. Takvi sistemi se zovu *Security Information and Event Management* (SIEM) sistemi.

II. IMPLEMENTACIJA SIEM SISTEMA

Implementacija SIEM sistema [2] zahtjeva prethodnu analizu i planiranje same implementacije. Pod analizom i planiranjem implementacije se podrazumijeva:

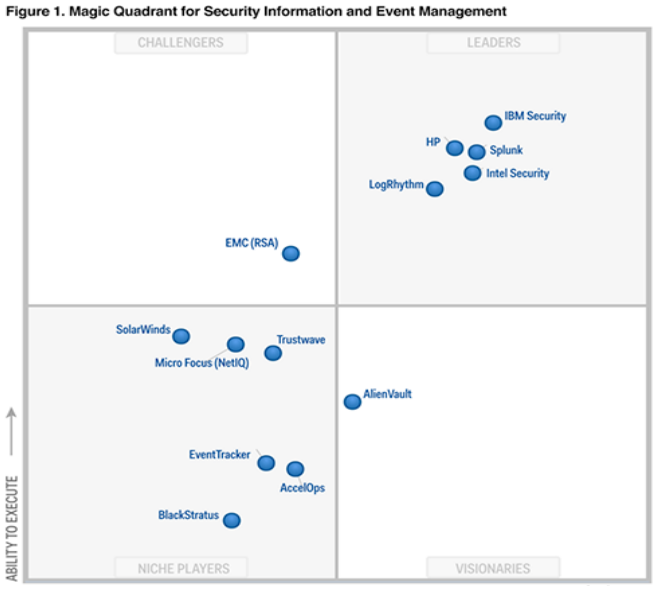
- definisanje sigurnosnih ciljeva kompanije,
- implementacija internih sigurnosnih politika koje tačno propisuju šta i u kojoj mjeri treba logovati na kojim sistemima odnosno koje izvještaje sigurnosnih sistema

i sistema za monitoring treba importovati u SIEM sistem da bi se realizovali sigurnosni ciljevi kompanije,

- definisanje vremenskog perioda čuvanja zapisa na SIEM sistemu u skladu sa sigurnosnim ciljevima kompanije i/ili zakonskom regulativom,
- određivanje srednjeg broj generisanih događaja po sekundi – *Events per Second* (EPS) po sistemu koji generiše podatke koji se žele prikupljati na SIEM sistemu (uzimaju se u obzir i planirana proširenja IT okruženja) i ukupnog broja EPS
- određivanje broja izvora (uzimaju se u obzir i planirana proširenja IT okruženja).

Na osnovu prethodno navedenih koraka analize i planiranja implementacije, vrši se dimenzionisanje sistema tako da se zadovolje zahtjevi za memorijskim prostorom potrebnim za smještanje podataka i njihovo čuvanje željeni vremenski period te da sistem bude dimenzionisan tako da podržava procesiranja određenog ukupnog broja EPS kao i željenog broja izvora podataka [3].

Kada je pravilno izvršeno dimenzionisanje sistema, najmanji problem predstavlja izbor sistema. Mnoge kompanije se prilikom izbora sistema vode Gartnerovim kvadratom. Na slici koja slijedi (Sl. 2) prikazan je Gartnerov kvadrat za SIEM za 2015. godinu. Nakon analize i planiranja implementacije i izbora sistema, slijedi faza implementacije. Prvo se, ukoliko već nije, konfiguriše logovanje na sistemima koji su planirani kao izvori logova a u skladu sa definisanih nivoom logovanja i selekcijom istih. Sistemi izvori se konfigurišu kao izvori i na strani SIEM sistema i ovim korakom je na SIEM sistemu završeno konfigurisanje automatizovanog centralizovanog prikupljanja podataka. SIEM vrši normalizaciju prikupljenih podataka različitih formata u unificirani format te je pretraživanje, analiziranje i filtriranje podataka vrlo jednostavno.

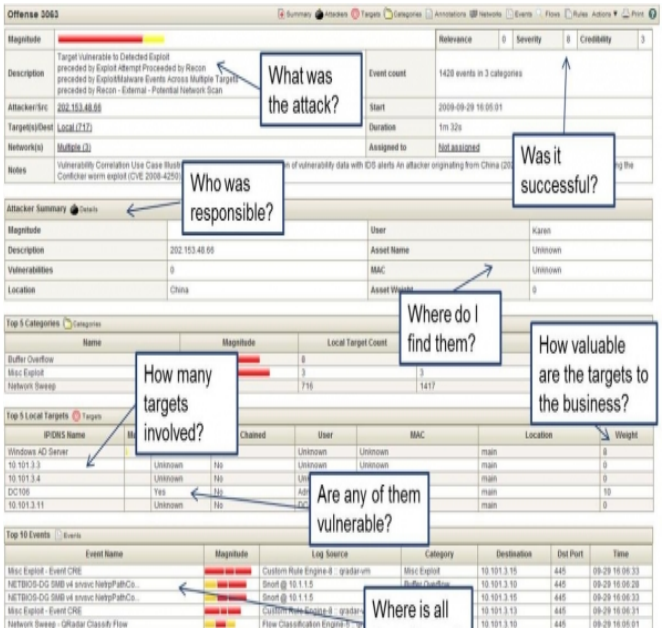


Slika 2. Gartnerov kvadrat za SIEM sistem za 2015. godinu [4]

Ključna funkcionalnost SIEM sistema jeste mogućnost automatizovanih korelacija prikupljanih podataka. Ova funkcionalnost predstavlja glavnu (ne i jedinu) razliku u odnosu na Log Management sistem koja SIEM čini superiornijim sistemom sa sigurnosnog aspekta. Korelacije podataka se vrše automatizovano i prema konfigurisanim pravilima. Kod kreiranja korelacionih pravila se vodi računa da rezultati korelacija vode ka već zadanom sigurnosnom cilju implementacije SIEM sistema. Ovo ujedno predstavlja i najzahtjevniji korak implementacije, zato što je korelaciona pravila potrebno konstantno poboljšavati na način da se smanjuje broj lažno pozitivnih rezultata korelacija i koriste odgovarajući pragovi tolerancije. Dakle, podešavanje korelacionih pravila nikad ne prestaje. Tim sigurnosnih stručnjaka, obučenih za rad na SIEM sistemu, konstantno prati nove sigurnosne prijetnji i potpise napada i konstantno kreira, analizira i poboljšava nova pravila. Proceduru kreiranja, analize i podešavanja korelacionih pravila je poželjno dokumentovati radi definisanja načina na koji se vrši tjuniranje korelacionih pravila. Isto tako je potrebno dokumentovati i rezultate korelacionih pravila (broj lažno pozitivnih upozorenja) jer oni služe za potvrdu poboljšanja korelacionih pravila (npr. smanjivanje broja lažno pozitivnih rezultata nakon tjuniranja korelacionog pravila) [5].

Svaki SIEM sistem ima set predefinisanih korelacionih pravila koja se koriste radi detekcije poznatih napada. U većini implementacija se ova predefinisana korelaciona pravila koriste i nakon implementacije ali sigurnosni tim konstantno radi na njihovoj analizi na sljedeći način: analiziraju se rezultati ovih korelacionih pravila sa ciljem isključivanja onih koja nisu u interesu sigurnosti konkretnog IT okruženja jer takva korelaciona pravila nepotrebno opterećuju SIEM sistem. Ona koja su od interesa za konkretno IT okruženje nastavljaju da se koriste ali se tjuniraju na isti način kao i ranije opisana posebno kreirana korelaciona pravila. Ukratko je opisan process kreiranja korelacionih pravila, analize predefinisanih korelacionih pravila i finog podešavanja istih što predstavlja najzahtjevniji korak implementacije SIEM sistema.

Drugi korak po zahtjevnosti jeste uspostavljanje procesa odgovaranja na alerte. SIEM, uz predefinisane algoritme za određivanje važnosti i kritičnosti rezultata korelacija, nudi i mogućnost podešavanja istih. Praksa pokazuje da je najbolje broj procesa odgovaranja na alerte svesti na najmanji mogući broj. Ukoliko već ne postoji primjenljiv proces odgovora na neki alert, kreira se novi. Dakle, idealno bi bilo smanjiti broj odgovora na alerte do granice postojanja procesa odgovora na svaki alert. Ovi procesi definišu šta je prihvatljivo "dobro" ponašanje, na šta treba odgovarati ili mijenjati. Potrebno je konstantno analizirati svaki alert, korelaciono pravilo koje ga generiše, skup događaja/aktivnosti koje dovode do generisanja alerta, razmotriti mogućnost lažno pozitivnog alerta te otkriti šta treba mijenjati kako se oni ne bi generisali. Ovdje važi zlatno pravilo: Više vremena provedenog na analizi jednog alerta znači manje vremena provedenog na analizi drugih alerta. Manje vremena provedenog na analizi jednog alerta znači više malicioznih aktivnosti koje ostaju neotkrivene (Sl. 3). Kada se uspostavi odgovarajući proces odgovora na alert isti treba dokumentovati na način da bude ponovljiv i dostupan svim članovima sigurnosnog tima.



Slika 3. Analiza alerta [6]

U tekstu koji slijedi opisan je jednostavan primjer prikupljanja podataka na SIEM sistemu, kreiranja korelacionog pravila, analize alerta i definisanja odgovora na mogući incident. Predstavljen je postupak uspostavljanja dinamičke liste korisnika Oracle baze podataka i praćenja novih legitimnih i sumnjivih korisnika. Podrazumijeva se da je audit na bazi podataka omogućen (npr. audit_trail=„DB“ – audit omogućen i svi audit podaci se čuvaju u bazi u sys.aud$ tabeli) kao i da je uključen audit svih logovanja na Oracle bazu podataka (komanda AUDIT SESSION;). Na strani SIEM sistema se, prema proceduri proizvođača, konfiguriše novi log izvor – Oracle baza podataka a zatim i prikupljanje audit podataka (zavisi od podržanih protokola - najčešće je potrebno kreirati nalog na bazi podataka kojim SIEM putem JDBC protokola pristupa dba_audit_trail). Nakon primjene gore navedenog SIEM se u realnom vremenu snabdijeva podacima potrebnim za uspostavljanje liste korisnika baze podataka. Referentna lista korisnika može biti ažurirana i od strane administratora i od strane korelacionog pravila. Korelaciono pravilo treba da provjerava sljedeće uslove: da je destinaciona IP adresa jednaka IP adresi servera baze podataka, da je log izvor baza podataka na tom serveru, da je naziv eventa jednak nazivu koji odgovara uspješnom logovanju (najčešće LOGON SUCCESSFUL) i da atribut eventa Username nije u referentnoj listi korisnika te baze podataka. Ukoliko su svi uslovi ispunjeni, istovremeno se trigeruje alert o novom korisniku i ažurira lista korisnika korisničkim imenom novog korisnika. Primjenom ovog korelacionog pravila, lista korisnika baze podataka se ažurira svaki put kada se novi korisnik uspješno loguje i trigeruje se alert o novom korisniku. Svaki alert treba da ima odgovarajući odgovor na alert. Sigurnosni tim koji analizira alerte treba da provjeri novog korisnika. U većem broju kompanija je uobičajeno da se podnosi zahtjev za kreiranje novog korisničkog naloga kao i da se poštuje propisana konvencija o imenovanju naloga ali i da se kreiranje naloga odobri putem telefona za potrebe hitne intervencije na bazi podataka. Nepostojanje odobrenog zahtjeva ili nepoštovanje konvencije o imenovanju naloga su najčešći indikatori sumnjivih naloga. Odgovor na ovaj alert zavisi od rezultata analiza a mogao bi biti onemogućenje sumnjivog naloga i brisanje korisničkog imena istog iz liste korisnika baze podataka ili samo preimenovanje naloga ili onemogućenje kompromitovanog naloga koji je kreirao ovaj nalog i svih naloga koji su kreirani kompromitovanim nalogom. Analizira se kako i zašto je nalog kreiran (zloupotreba administratorskih privilegija, kompromitovanje privilegovanog naloga i kreiranje novih naloga upotrebom istog, nepoštovanje propisane procedure kreiranja naloga izostavljanjem zahtjeva itd.), koje privilegije su dodjeljene blokiranom nalogu, koje aktivnosti su uspješno izvršene sumnjivim nalogom od trenutka logovanja do momenta blokiranja i slično.

Za primjer automatizovane provjere postojanja odobrenog zahtjeva za kreiranje naloga novog korisnika koji se uspješno logovao u bazu podataka treba kreirati korelaciono pravilo i referentnu listu odobrenih zahtjeva. U ovom slučaju se referentna lista popunjava od strane administratora koji po prijemu zahtjeva unosi username naloga u referentnu listu i kreira nalog za novog korisnika u bazi podataka. Korelaciono pravilo ima sve uslove prethodno opisanog pravila uz dodatni uslov – da se username ne nalazi na referentnoj listi odobrenih zahtjeva za kreiranje. Ukoliko su svi uslovi ispunjeni trigeruje se alert. Odgovor na alert bi trebao biti blokiranje naloga kao u prethodnom primjeru. Dakle, ovo korelaciono pravilo trigeruje alert u slučaju da se novi korisnik koji nije na listi korisnika baze podataka (lista iz prethodnog primjera) uspješno logovao na bazu podataka a da ne postoji odobren zahtjev za kreiranje naloga za novog korisnika. Primjena ovog korelacionog pravila zahtjeva redovno ažuriranje referentne liste odobrenih zahtjeva za kreiranje naloga u bazi podataka. U suprotnom bi jedan broj alerta bio lažno pozitivan. Primjena odgovora na alert koji trigeruje ovo pravilo bi onemogućila rad legitimnih korisnika baze podataka ukoliko administrator nije ažurirao referentnu listu odobrenih zahtjeva. Primjena ovog korelacionog pravila je sigurno poželjna u ISO27001 standardizovanim okruženjima. Oba, prethodno opisana, primjera su primjenljiva u gotovo svim okruženjima.

III. OPTIMIZACIJA IMPLEMENTACIJE SIEM SISTEMA

Mnoge implementacije kojima nije prethodila analiza i planiranje nisu dale pozitivan sigurnosni rezultat niti doprinose višem stepenu sigurnosti IT okruženja te se mogućnost optimizacije implementacije SIEM sistema nazire već u ovoj fazi. Analiza i planiranje ne samo da olakšavaju implementaciju nego su neophodne za dobro dimenzionisanje sistema. Ukoliko se ne izvrši dobra procjena potreba okruženja po pitanju ukupnog broja EPS ili memorijskog prostoru, može se desiti da sistem ne može procesirati dovoljan broj EPS koji se generiše u korporativnoj mreži ili ne može ispuniti zahtjeve

zakona ili interne sigurnosne politike po pitanju vremenskog perioda čuvanja prikupljenih podataka.

Moguća je i ušteda kada je u pitanju licenca SIEM sistema vezano za broj log izvora sa kojih se prikupljaju podaci. SIEM sistemi se najčešće licenciraju, osim po broju EPS, i po broju log izvora sa kojih se prikupljaju podaci. IT okruženja obično i prije implementacije SIEM sistema imaju implementiran ili Log Management sistem ili neki syslog server na koji se syslog protokolom šalju logovi sa mrežnih uređaja. Neka jedan takav syslog server prikuplja logove sa 300 mrežnih uređaja. Ako se syslog server posmatra kao jedan log izvor onda se po jednom log izvoru dobijaju na SIEM-u logovi sa 300 mrežnih uređaja a ako se svaki od tih uređaja posmatra kao poseban log izvor onda SIEM sistem raspolaže istim podacima ali je odgovarajuća licenca mnogo skuplja. Ovo sve zavisi od licencne metrike proizvođača SIEM sistema jer je kod nekih proizvođača moguće na ovaj način ostvariti veliku uštedu dok drugi proizvođači licenciraju sistem baš po broju krajnjih uređaja.

Ušteda se ostvaruje i kada se iskoristi već postojeći Log Management sistema i implementira samo nadogradnja ovog sistema koja ima sve ključne funkcionalnosti SIEM sistema. Jedan od takvih SIEM sistema je ArcSight Express. Ukoliko je nadogradnja Log Management sistema moguća, onda se dobija ne samo mogućnost uštede nego i znatno jednostavnija implementacija. Planiranje Log Managementa je veoma slično implementaciji SIEM sistema i smatra se da su u takvim okruženjima već definisani sistemi izvori kao i logovi od interesa. Iskustvo u radu sa Log Management sistemom i sama potreba okruženja za nadogradnjom postojećeg sistema, ukazuje na to da je okruženje "zrelo" za implementaciju SIEM sistema i da se unaprijed zna šta bi bio njegov zadatak. Sigurnosni stručnjaci čak preporučuju ovakav način implementacije SIEM sistema, korak po korak, od Log Management sistema do SIEM sistem.

Za dobre analize podataka potrebno je obezbjediti podatke odnosno snabdjevati SIEM sistem što većom količinom podataka od interesa. Ovdje važi pravilo "što više raspoloživih podataka to su bolje analize istih".

Da bi implementacija SIEM sistema ostvarila unaprijed postavljene sigurnosne ciljeve potrebno je vrijeme. Koliko god implementacija SIEM sistema bila jednostavna na prvi pogled treba znati da je to samo inicijalna implementacija koja podrazumijeva lociranje uređaja u mrežu, konfigurisanje osnovnih mrežnih parametara i prikupljanje logova sa sistema iz mreže. Implementacija koja ima za cilj podizanje nivoa sigurnosti u mrežnom okruženju ne prestaje nikad. Podešavanje korelacionih pravila je iterativan postupak i analizom rezultata kreiranih korelacija konstantno se otkrivaju načini za smanjivanjem broja lažno pozitivnih/negativnih rezultata. Kada se korelaciono pravilo kreira, jedno vrijeme se analiziraju rezultati ovih korelacija, zatim se vrši fino podešavanje istih kako bi se smanjio broj lažno pozitivnih rezultata i fino podesili odgovarajući pragovi korelacija. Pragovi mogu biti previsoki što rezultuje tim da stvarni napad može proći neopaženo dok preniski pragovi rezultuju velikim brojem uglavnom lažno pozitivnih alerta. Sigurnosni tim ima zadatak da prati najnovije prijetnje, a sa novim prijetnjama i modelom novih napada, potrebno je kreirati i nova korelaciona pravila ili podešavati već kreirana kako bi se detektovale nove vrste napada ili sumnjivih aktivnosti.

IV. UTICAJ LJUDSKOG FAKTORA NA IMPLEMENTACIJU SIEM SISTEMA

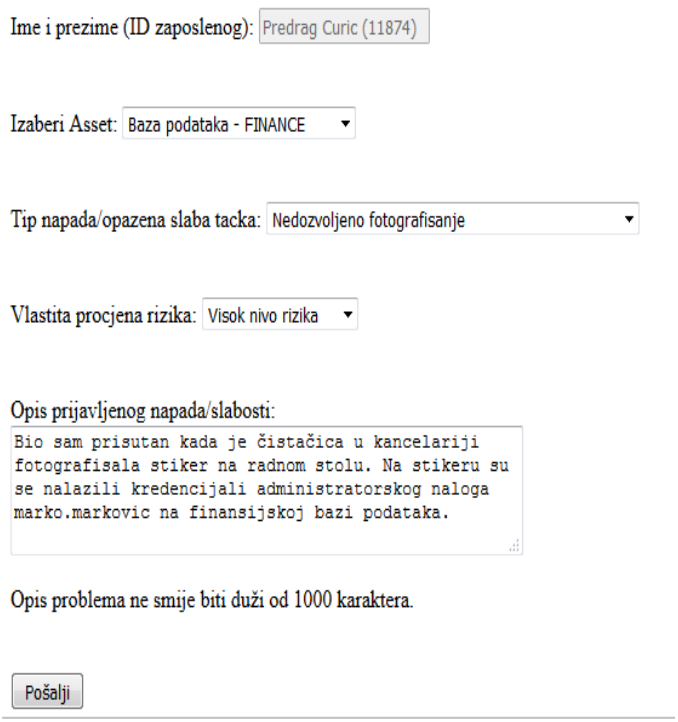
Prethodno opisana implementacija zahtjeva neprekidnu angažovanost sigurnosnog tima te je uticaj ljudskog faktora evidentan. Bez obzira na činjenicu da SIEM predstavlja sistem koji vrši automatizovane korelacije i željene detekcije, ovaj sistem može detektovati napade samo na osnovu analize podataka prikupljanih sa IT sistema. Međutim, današnji hakeri izvršavaju napade kombinovanjem raznih ranjivosti uključujući i socijalni inženjering pa i fizički pristup IT sistemima. Ovakve napade SIEM ne može da detektuje jer analizira samo podatke prikupljene sa IT sistema ne uključujući ljudsku inteligenciju ili opažanja. SIEM ne raspolaže informacijama koje ljudi mogu primjetiti npr. o tome da je neki službeni laptop ili mobilni telefon sa povjerljivim podacima i kredencijalima ukraden ili izgubljen ili da je neko pokušao saznati lozinku nekog sistema u razgovoru sa administratorima.

Standard ISO/IEC 27001 obuhvata ljudske resurse, upravljanje zapisima, neprekidnost poslovanja i upravljanje rizikom (A.13.1 – *Information Security Incident Management*; A.13.1.1 – *Reporting information security events and weaknesses*; A13.1.2 – *Reporting security weaknesses* itd). Implementacija SIEM sistema ispunjava zahtjeve standarda i doprinosi njegovoj implementaciji. Dolazi se do zaključka da bi SIEM, iako ima ugrađenu visoku inteligenciju, dao najbolje sigurnosne rezultate u kombinaciji sa ljudskim opažanjima. Postavlja se pitanje kako SIEM sistemu dostaviti informacije koje čovjek može zaključiti ili primjetiti. Nije nemoguce razviti interfejs koji omogućava snabdijevanje SIEM sistema sigurnosnim informacijama koje su rezultat ljudskog opažanja ili razmišljanja. Npr. naizgled bezopasan telefonski poziv nepoznate osobe koja hitno traži lozinku za pristup nekom IT sistemu bi mogao biti dobar ulazni podatak SIEM sistemu radi dodatne analize sigurnosti tog sistema. Ukoliko dodatno *firewall* i *Intrusion Detection System* (IDS) pokazuju više malicioznih aktivnosti usmjerenih na taj sistem podiže se nivo kritičnosti tog alerta. Ovo je samo jedan jednostavan primjer detekcije zlonamjernih aktivnosti gdje je ulazni podatak ljudsko opažanje.

Brojne su zloupotrebe koje u početku samo čovjeku mogu biti sumnjive a kasnijom dodatnom analizom se može potvrditi da nisu samo sumnjive nego i zlonamjerne. Sve *on-site* posjete, kao i održavanja IT sistema kompanije od strane lica koja nisu zaposlena u kompaniji i imaju ugovor o održavanju istih mogu biti sumnjiva. Kada se zna da zaposleni drže stiker sa lozinkom za pristup nekom IT sistemu na vidljivom mjestu u kancelariji, sumnjive mogu biti i čistačice i sekretarice i svi koji ulaze u tu kancelariju. Ali sve nabrojano nije moguće detektovati SIEM sistemom ukoliko se ne razvije dodatni interfejs za unos podataka te vrste. Ljudi su veoma često odlični detektori neuobičajenih aktivnosti i mogućih zloupotreba. U velikom broju slučajeva oni nemaju kome prijaviti uočeno ili se ustručavaju da to urade. Razlozi za ustručavanje zaposlenih vezano za prijavljivanje sumnjivih aktivnosti su brojni: svoju sumnjičavost smatraju nebitnom, strah od ismijavanja od strane

sigurnosnog tima, strah od negativnih posljedica ili kažnjavanja, nelagoda pri pomisli da su prijavili ili osumnjičili pogrešnu osobu i slično. Ukoliko bi se razvio interfejs za unos podataka ove vrste i dobro definisali načini na koji se oni unose/prijavljuju kao i edukovali zaposleni o značaju njihove uključenosti u podizanje nivoa sigurnosti IT okruženja, zaposleni bi bili ohrabreni da prijavljuju ovakve slučajeve a inteligentni SIEM sistemi bi bili obogaćeni i ljudskom inteligencijom što bi sigurno rezultovalo višim nivoom sigurnosti IT okruženja.

Razvijanje ovakvog interfejsa za SIEM sistem je bila jedna od tema obrađenih na *RSA conference 2014* održanom u San Francisku [7] a u ovom radu se koristi samo kao jedna od smjernica za optimizaciju implementacije SIEM sistema i maksimalnu iskoristivost ovih inteligentnih sistema. Razvijanje ovih interfejsa zahtjeva opširnu analizu i planiranje. Da bi se napravio model rada interfejsa potrebno je prethodno istražiti načine na koje čovjek može uticati na sigurnost informacionog sistema, te razmotriti koja grupa zaposlenih je najkritičnija po pitanju manipulacija vezanih za pristup informacionim sistemima te definisati vektore kombinovanih napada koji se trebaju nadgledati. Dizajniranje web aplikacije koja generiše željene logove dolazi na kraju. Najjednostavnija aplikacija bi trebala da ponudi korisniku mogućnost izbora unaprijed definisanih sistema od interesa (npr. baza ličnih podataka), zatim izbora kombinovanog napada koji se može prijaviti, te mogućnost procjene nivoa rizika kao i opciono dodavanje opisa. Aplikacija bi kao izlaz trebala da generiše log zapis koji se šalje SIEM sistemu, koji sve logove čuva na centralizovanoj lokaciji, na korelacije sa ostalim logovima i sigurnosnim informacijama radi detekcije napada.



Slika 4. Korisnički interfejs za unos podataka

V. ZAKLJUČAK

Brojne funkcionalnosti SIEM sistema znatno olakšavaju posao svakog administratora pojedinačno jer se implementacijom navedenog sistema svi logovi prikupljaju, analiziraju i korelišu na centralizovanoj lokaciji. Evidentno je da veliki uticaj na uspješnost implementacije ima ljudski faktor – stručnost i kompetentnost sigurnosnog tima, edukacija svih zaposlenih, posvećenost sigurnosnog tima podešavanju korelacionih pravila i uspostavljanju mehanizma odgovaranja na incidente i sama ljudska opažanja u vezi IT sigurnosti. Korelacija ljudskih opažanja i podataka kojima SIEM sistemi raspolažu je takođe moguća. Razvojem aplikaciju kao SIEM interfejsa za unos logova koji nose informacije o ljudskim opažanjima dobija se puno na polju sigurnosti cjelokupnog IT okruženja i pokriva se dio detekcije netehničkih prijetnji i slabosti svakog okruženja. Netehničke prijetnje i napade je veoma teško detektovati i precesuirati, pogotovo sistemima, te mogućnost automatizovanih korelacija ljudskih opažanja i sigurnosnih podataka koje generišu svi sistemi IT okruženja doprinosi cjelokupnoj sigurnosti IT okruženja.

LITERATURA

[1] Aleksandar Radosavljević, Srđan Milojević, Arcsight Solution for Log Management – Case Study of Information System by Telekom Srbija, S&T Serbia, Beograd, IDC IT Security and Datacenters Transformation Roadshow 2011, dostupno na: http://idcrussia.com/ru/events/39016-idc-it-security-and-datacenters-transformation-roadshow-2011/10-agenda , posjećeno: 03.01.2016. godine

[2] David R. Miller, Shon Harris, Allen A. Harper, Stephen VanDyke, Chris Blask, Security Information and Event Management (SIEM) Implementation, NewYork: McGraw-Hill 2011

[3] J. Michael Butler, Benchmarking Security Information and Event Management (SIEM), SANS whitepaper, 2009

[4] Haiyan Song, Get Two Gartner Reports: The 2015 Magic Quadrant and the 2015 Critical Capabilities for SIEM to See Why Splunk Was Named a Leader for the Third Straight Year, 2015, dostupno na http://www.splunk.com/goto/SIEM_MQ , posjećeno 03.01.2016. godine

[5] Anthon Chuvakin, SIEM Use Case Implementation and Tuning Process, November 2015, dostupno na Gartner Blog Network: http://blogs.gartner.com/anton-chuvakin/2015/11/25/siem-use-case-implementation-and-tuning-process/ , posjećeno 03.01.2016. godine

[6] Marc van Zadelhoff, Brian Mulligan, IBM Security systems – Disrupt the Advanced Attack Chain with Intelligent, Integrated Security, Security Inteligence: Think Integrated, November 2013, dostupno na http://www.slideshare.net/ibmsecurity/disrupt-the-advanced-attack-chain-with-intelligent-integrated-security , posjećeno 03.01.2016. godine

[7] Bettina Wesselmann, Johannes Wiele, A Human Factor Interface for SIEM, San Francisco, RSA CONFERENCE, 2014, dostupno na: http://www.rsaconference.com/events/us14/agenda/sessions/935/a-human-factor-interface-for-siem , posjećeno 03.01.2016. godine

ABSTRACT

These papers describe the process of implementation of Security Information Event Management (SIEM) systems in the IT environment and the impact of human factor on that process. In the introductory part are listed the most often used security systems in corporate IT environments, key functionality of the SIEM systems and its importance in the overall security of the IT environments. Then, it is suggested recommendations for the successful implementation of the SIEM systems which aims higher level of security of corporate network environment. Next, it is presented optimization of the implementation of the SIEM systems through all its phases.

Then, it is described the impact of human factor on the implementation of these systems as well as the impact of human observations in correlations to attack detection.

THE IMAPCT OF HUMAN FACTOR IN IMPLEMENTATION OF SIEM SISTEMS

Bojana Vilendecic, Ratko Dejanovic, Predrag Curic