UNIVERZA V LJUBLJANI
FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Tomaž Hiti

Odločitveni model uvedbe sistema za upravljanje varnostnih informacij in dogodkov

MAGISTRSKO DELO

mentor: prof. dr. Marko Bajec

Ljubljana, 2011

Univerza
v Ljubljani

Fakulteta za računalništvo
in informatiko

Tržaška 25
1000 Ljubljana, Slovenija
telefon: 01 476 84 11
faks: 01 426 46 47
www.fri.uni-lj.si
e-mail: dekanat@fri.uni-lj.si

Št.: 141-MAG-RI/2011
Datum: 27. 05. 2011

Tomaž HITI, univ. dipl. inž. rač. in inf.

Ljubljana

Fakulteta za računalništvo in informatiko Univerze v Ljubljani izdaja naslednjo magistrsko nalogo

Naslov naloge: **Odločitveni model uvedbe sistema za upravljanje varnostnih informacij in dogodkov**

Decision model for implementing a security information and event management system

Tematika naloge:

V okviru magistrskega dela podrobneje izdelajte odločitveni model postavitve sistema za upravljanje varnostnih informacij in dogodkov (angl. Security Information and Event Management – SIEM). Podrobneje predstavite različne tipe arhitekturnih rešitev, ter izpostavite njihove prednosti in slabosti. Model naj bo zasnovan na podlagi rezultatov in pridobljenih izkušenj, ki ste jih osvojili tekom implementacije SIEM sistema v banki. Ker gre za vpeljevanje nove storitve v informacijski sistem, pri tem upoštevajte dobre prakse ITIL (angl. IT Infrastructure Library) in COBIT (angl. Control Objectives for Information and related Technology). V praktičnem delu naloge prikažite zmogljivosti takega sistema: zajem dnevniških zapisov, primer korelacije, obveščanje o incidentih in kršitvah, izdelavo osnovnih varnostnih poročil in izdelavo poročila o skladnosti s standardi.

Mentor:

prof. dr. Marko Bajec

Fakulteta za računalništvo in informatiko • UNIVERZA V LJUBLJANI • 2

Dekan:

prof. dr. Nikolaj Zimic

I Z J A V A O A V T O R S T V U

magistrskega dela

Spodaj podpisani/-a Tomaž Hiti,

z vpisno številko 63980047,

sem avtor magistrskega dela z naslovom

Odločitveni model uvedbe sistema za upravljanje varnostnih informacij in dogodkov

S svojim podpisom zagotavljam, da:

- sem magistrsko delo izdelal samostojno pod vodstvom mentorja (naziv, ime in priimek)

  prof. dr. Marko Bajec

  in somentorstvom (naziv, ime in priimek)

- so elektronska oblika magistrskega dela, naslova (slov., angl.), povzetka (slov., angl.) ter ključne besede (slov., angl.) identični s tiskano obliko magistrskega dela

- in soglašam z javno objavo elektronske oblike magistrskega dela v zbirki »Dela FRI«.

V Ljubljani, dne _____ Podpis avtorja: _____

ZAHVALA

Zahvaljujem se mentorju, prof. dr. Marku Bajcu za strokovne nasvete in priporočila pri izdelavi magistrske naloge.
Hvala staršem, Poloni in vsem, ki so verjeli vame.

Kazalo

Povzetek 1
Abstract 2
1. Uvod 3
1.1 Opredelitev problema in cilji naloge 3
1.2 Struktura magistrske naloge 3
2. Varovanje informacij 5
2.1 Zagotavljanja informacijske varnosti 6
2.1.1 Sistem upravljanja varovanja informacij 6
2.2 Standardi družine ISO/IEC 27000 8
2.2.1 ISO/IEC 27001 10
2.2.2 ISO/IEC 27002 11
2.3 ITIL 11
2.4 COBIT 20
3. Upravljanje varnostnih informacij in dogodkov 22
3.1 Osnovni pojmi 22
3.2 Upravljanje varnostnih informacij 23
3.3 Upravljanje varnostnih dogodkov 23
3.4 Upravljanje varnostnih informacij in dogodkov 24
4. Opis delovanja sistema SIEM 28
4.1 Splošno 28
4.2 SIEM arhitektura 28
4.3 Format, transport in vsebina dnevnika 34
4.3.1 Format 34
4.3.2 Transport 36
4.3.3 Vsebina 37
4.3.4 Nove smernice 37
5. Vzpostavitev sistema SIEM 41
5.1 Razlogi za SIEM 41
5.2 Postopki pred vzpostavitvijo 42
5.2.1 Organizacija 42
5.2.1.1 Vloge 42
5.2.2 Produkt 43
5.2.3 Proizvajalec 43
5.2.4 Omrežje 44
5.3 Zagotavljanja varnosti 45

5.4 Viri ... 46
5.5 Namestitev ... 48
5.6 Najbolj pogoste napake ... 49
6. Odločitveni model ... 50
6.1 Identifikacija odločitvenega problema ... 53
6.1.1 Analiza stanja ... 54
6.1.2 Zrelost procesov ... 55
6.2 Identifikacija različic ... 57
6.3 Razgradnja problema in modeliranje ... 59
6.4 Vrednotenje, analiza in izbira različic ... 62
6.4.1 ArcSight ... 62
6.4.2 RSA (EMC) ... 66
6.4.3 CA ... 67
6.4.4 Vrednotenje ... 68
6.5 Realizacija odločitve ... 71
6.6 Gartnerjeva analiza ... 72
7. Sklepne ugotovitve ... 75
PRILOGA – Praktični del ... 76
Seznam slik ... 78
Seznam tabel ... 78
Viri ... 79

Seznam kratic

API	Application Programming Interface (slov. vmesnik za programiranje aplikacij)
CCTA	Central Computer and Telecommunications Agency (slov. centralna agencija za komunikacije in telekomunikacije)
COBIT	Control Objectives for Information and related Technology (slov. kontrolni cilji za informacijsko in sorodno tehnologijo)
DBMS	Database Management Systems (slov. sistem za upravljanje podatkovnih baz)
DLP	Data Loss Prevention (slov. preprečevanje izgube podatkov)
DMZ	Demilitarized Zone (slov. demilitarizirano območje)
ERP	Enterprise Resource Planning (slov. načrtovanje virov podjetja)
FIM	File Integrity Monitoring (slov. nadzor integritete datotek)
GLBA	Gamm-Leach-Bileley Act (slov. zakon o modernizaciji finančnih servisov)
HIPAA	Helth Insurance Portability and Accountability Act (slov. zakon zdravstvenega zavarovanja, prenosljivosti in odgovornosti)
IdM	Identity Management (slov. upravljanje identitet)
IDS	Intrusion Detection System (slov. sistem za zaznavanje vdorov)
IPS	Intrusion Prevention System (slov. sistem za preprečevanje vdorov)
ISO	International Organization for Standardization (slov. mednarodna organizacija za standardizacijo)
ITIL	Information Technology Infrastructure Library (slov. priporočila za upravljanje in uvajanje storitev IT)
KPI	Key Performance Indicators (slov. ključni kazalniki delovanja)
LAN	Local Area Network (slov. lokalno ali krajevno omrežje)
NIST	National Institute of Standards and Technology (slov. nacionalni inštitut za tehnologijo in standarde)
OGC	Office of Government Commerce (slov. britanski trgovinski urad)
OSI	Open System Interconnection (slov. odprti sistem povezovanja)
PCI DSS	Payment Card Industry Data Security Standard (slov. standard za varovanje podatkov v industriji plačilnih kartic)
PMF	Process Maturity Framework (slov. zrelostni model procesov upravljanja storitev)
RFC	Request for Comments (slov. prošnja za pripombe/komentarje)
SEM	Security Event Management (slov. upravljanje varnostnih dogodkov)
SIEM	Security Information and Event Management (slov. upravljanje varnostnih informacij in dogodkov)
SIM	Security Information Management (slov. upravljanje varnostnih informacij)
SIST	Slovenski inštitut za standardizacijo
SNMP	Simple Network Management Protocol (slov. preprost protokol za upravljanje omrežja)
SOAP	Simple Object Access Protocol (standard za spletne storitve, ki temelji na XML)
SQL	Structured Query Language (slov. strukturiran povpraševalni jezik za delo s podatkovnimi bazami)
SSH	Secure Shell (slov. varna lupina)
SUVI	Sistem za upravljanje varovanja informacij
SWOT	Strengths, Weaknesses, Opportunities, Threats (slov. analiza prednosti, slabosti, priložnosti in nevarnosti)
TCP	Transmission Control Protocol (slov. protokol za nadzor transporta)
UDP	User Data Protocol (slov. uporabniški datagramski protokol)
XML	eXtensible Markup Language (slov. razširljivi označevalni jezik)

Povzetek

Odločitveni model uvedbe sistema za upravljanje varnostnih informacij in dogodkov

Organizacije se vedno bolj zavedajo pomembnosti zagotavljanja ustrezne informacijske varnosti. Motivatorjev za to je več, med drugim varovanje zaupnih podatkov, upoštevanje zakonskih regulativ na tem področju in podobno. Poleg tega so sodobni informacijski sistemi vedno bolj kompleksni in izpostavljeni raznim grožnjam. Omenjeno posledično pomeni generiranje ogromne količine informacij in dogodkov, ki so pogostokrat razpršeni po posameznih sistemih. Za kakovostno obvladovanje na posameznih sistemih je nujno potrebno centralizirano upravljanje dogodkov. Slednjega se v banki zavedamo in smo zato pristopili k iskanju ustrezne rešitve na področju upravljanja varnostnih informacij in dogodkov (SIEM).

V pričujočem delu smo predlagali odločitveni model za izbiro sistema za upravljanje varnostnih informacij in dogodkov. Namen magistrskega dela je olajšati proces odločanja oz. izbiro sistema SIEM. V želji, da bi bil proces odločanja čim bolj realen, smo s tremi ponudniki SIEM rešitev izvedli pilotsko postavitev. Pri ocenjevanju posameznih različic smo izpostavili njihove prednosti in slabosti ter predstavili posamezne arhitekturne rešitve. Za proces odločanja najustreznejše različice smo uporabili metodo uteži parametrov, ki spada v skupino večparametrskega ali večkriterijskega odločanja. Najboljšo oceno je dosegel sistem ArcSight, za katerega je predlagana končna arhitekturna rešitev. Končna rešitev temelji na postavitvi visoko razpoložljive konfiguracije z zagotavljanjem geografske redundance.

Opisani postopek odločanja je zasnovan tako, da je ponovljiv in uporaben tudi za druga podjetja oz. odločevalce. Ne glede na izbrane ponudnike lahko odločevalec izbere poljubne SIEM ponudnike in uporabi opisano metodologijo.

Ključne besede: upravljanje varnostnih informacij in dogodkov, upravljanje dnevnikov, odločitveni model, informacijska varnost, SIEM.

Abstract

Decision model for implementing a security information and event management system

Organizations are aware of the importance of adequate information security due to various reasons like protection of confidential data based on regulations and legislation. On the other hand modern information systems are becoming very complex and vulnerable, which causes the generation of enormous amount of information and events spread over the systems. Quality management system therefore requires centralized event management. In the bank we are aware of the problem and are looking forward to finding a solution in the field of information and event security management (SIEM).

In the present thesis the decision-making model for the choice of security information and event management is presented. The objective of the thesis is to facilitate the decision-making and the choice of appropriate SIEM; therefore three SIEM offers were chosen to present the pilot installation. The assessment of varieties was based on advantages and disadvantages as well as on architectural solutions. The process of decision-making was based on weight parameter estimation method which belongs to the group of multi-parameter and multi-criteria decision-making. The best results were obtained by ArcSight system for which the final architectural solution was proposed. The final solution is based on high geographic redundancy configuration.

The above decision-making process could be repeated and used by diverse enterprises or decision-makers. Despite the chosen offerer the decision-maker can choose any SIEM offerer and use the above methodology.

Key words: security information and event management, log management, decision model, information security, SIEM.

1. Uvod

Strateški informacijski sistemi so za banko ključnega pomena. Ti podpirajo strateško upravljanje poslovnih sistemov za doseganje konkurenčne prednosti na trgu. Za slednje so nujne naložbe v napredno strojno in programsko opremo. Poleg konkurenčne prednosti je za podjetje ključnega pomena zagotavljanje ustrezne informacijske varnosti [9], bodisi iz naslova varovanja informacij svojih komitentov, bodisi ker to velevajo vse strožje zakonske regulative.

Informacijski sistem banke je kompleksen in večplasten sistem, ki dnevno ustvari veliko količino informacij in dogodkov. Vse zbrane informacije nam brez naprednega centraliziranega upravljanja in korelacijskih mehanizmov omogočajo le delno seznanitev z dejanskimi grožnjami, napadi ter kršitvami znotraj sistemov. Za kakovostno obvladovanje dogodkov, ki se izvajajo na posameznih sistemih, je nujno potrebno centralizirano obravnavanje le teh [11]. Slednjega se v banki zavedamo in zato smo pristopili k iskanju ustrezne rešitve na področju upravljanja varnostnih informacij in dogodkov (angl. Security Information and Event Management).

1.1 Opredelitev problema in cilji naloge

Informacijski sistem (v nadaljevanju IS) podjetja je kompleksen in večplasten. Lokacijska razpršenost še dodatno zvišuje nivo kompleksnosti. V IS so bile vpeljane določene varnostne rešitve (IDS/IPS, preverjanje pristnosti 802.1x, segmentacija omrežja idr.) z namenom zagotavljanja višje stopnje informacijske varnosti. Težava nastopi, ker ima vsak od teh produktov svojo centralno konzolo, ki so med seboj nepovezane. Naslednja težava je v tem, da skrbniki nimajo celotnega pregleda nad dogajanjem v IS in s težavo nadzorujejo učinkovitost varnostnih ukrepov ter ustrezno informacijsko varnost. Omenjeno predstavlja še dodaten razlog, da je podjetje pristopilo k iskanju ustrezne rešitve za centralizirano upravljanje dnevnikov in dogodkov. Uporabljen pristop bi lahko razdelili v dva sklopa. Prvi zajema začetno izbiro SIEM ponudnikov s katerimi bi opravili testno postavitev, drugi pa testiranje postavljenega sistema SIEM ter proces odločanja najustreznejše različice.

Glavni cilj magistrske naloge je postavitev odločitvenega modela za izbiro sistema SIEM. Odločitev bo zasnovana na podlagi pridobljenih izkušenj pri pilotski postavitvi rešitve SIEM in samostojnega raziskovalnega dela. Opisani postopek odločanja je zasnovan tako, da je ponovljiv in uporaben tudi za druga podjetja oz. odločevalce. Ne glede na izbrane ponudnike, lahko odločevalec izbere poljubne SIEM ponudnike in uporabi opisano metodologijo.

1.2 Struktura magistrske naloge

Najprej bomo razčlenili področje varovanja informacij in določili glavni razlog, da podjetje sploh začne razmišljati o upravljanju varnostnih informacij in dogodkov. Ker gre pri vpeljavi rešitve SIEM v IS za novo storitev, bodo pri tem upoštevane dobre prakse ITIL [14]. V nadaljevanju bodo predstavljene bistvene značilnosti posameznih metodologij in standardov s področja upravljanja storitev IT. V tretjem poglavju bo podrobneje predstavljeno področje upravljanja varnostnih informacij in dogodkov. Seznanili se bomo s postopnim razvojem tega

področja ter vse večjim zanimanjem za njegovo vzpostavitev. V četrtem poglavju je podan opis glavnih funkcij in delovanja sistema SIEM. V nadaljevanju sledi pregled formatov, ki se uporabljajo na tem področju in seznanitev z novimi smernicami standardizacije. V petem poglavju bomo razdelali vzpostavitev sistema SIEM. Izpostavili bomo oba glavna razloga odločitev podjetij za vpeljavo rešitve SIEM: zagotavljanje skladnosti in obvladovanje groženj. Ker vzpostavitev sistema SIEM predstavlja kompleksen projekt, bomo v nadaljevanju podali osnovne smernice, ki jih je priporočljivo upoštevati pred vzpostavitvijo sistema SIEM. Na koncu poglavja bomo opozorili na deset najbolj pogostih napak, ki se dogajajo pri implementaciji sistema SIEM. V šestem poglavju bo predstavljen odločitveni model za izbor rešitve SIEM, ki je zasnovan na podlagi pridobljenih izkušenj in rezultatov vrednotenja oz. ocenjevanja različic. S tem želimo olajšati delo vsem, ki se bodo lotili implementacije sistema SIEM. Odločitveni proces bo potekal v petih fazah. Predstavljena bo analiza stanja današnjega bančnega upravljanja z varnostnimi informacijami in dogodki. Sledila bo identifikacija ponudnikov sistemov SIEM ter vrednotenje treh izbranih ponudnikov: ArcSight, RSA in CA. Podrobneje bomo predstavili različne tipe arhitekturnih rešitev ter izpostavili njihove prednosti in slabosti. Da bi bila odločitev pri izbiri SIEM ponudnikov lažja, smo v zaključku šestega poglavja podali povzetek Gartnerjeve analize petnajstih SIEM produktov. Sedmo poglavje predstavlja zaključek magistrskega dela.

2. Varovanje informacij

Varnost
Varnost kot poslovna kategorija predstavlja ocenjeno razmerje med sprejetimi tveganji za izpad poslovanja in vloženimi sredstvi za njegovo ohranitev in izboljšanje. Varni smo torej ob ugotovitvi, da nam tveganje neke grožnje lahko povzroči škodo, relativno sprejemljivo.

S ponovljivo metodo moramo znati oceniti vpliv morebitne grožnje na posamezno storitev oz. proces. Ocena predstavlja njegovo ranljivost in hkrati naše tveganje. Slednjo lahko zmanjšamo s protiukrepi oz. kontrolami. V primeru, da je tveganje majhno, ga sprejmemo. Če pa je potreben vložek v kontrole večji od tveganja, običajno dodatni ukrepi niso smiselni. Vsak velik vložek je potrebno še enkrat pretehtati in izjemoma kakšno tveganje tudi sprejeti brez dodatnih ukrepov. Postopek ugotavljanja tveganja imenujemo analiza/ocena tveganj (angl. risk analysis), ugotavljanje potrebnih in možnih ukrepov pa upravljanje s tveganji (angl. risk management).

Informacijska varnost (angl. information security)
Tako kot varnost ima tudi informacija veliko različnih definicij. Vidmar razlaga informacijo kot rezultat interpretacije podatkov [15]. Informacija je rezultat procesiranja, upravljanja in organiziranja podatkov na način, ki prejemniku informacije omogoča boljše razumevanje in poznavanje določene tematike. Prejemnik informacije nato interpretira informacijo v skladu s svojimi interesi. Na podlagi te interpretacije pa tudi sprejme odločitev, ki ga vodijo k določenemu dejanju. Informacije imajo lahko različne oblike, npr.: lahko so natisnjene, napisane na papir, v elektronski obliki, v obliki govora idr. oblike.

Informacijska varnost pomeni varovanje informacij in IS pred nesrečami, namerno škodo ali naravnimi katastrofami. To je neprekinjena dejavnost, ki traja 24/7. Vodstvo je odgovorno za postavitev temeljne varnostne politike. Razumeti mora kaj ščiti in zakaj ter določiti višino sredstev, ki jih je pripravljeno vložiti v varnostne ukrepe.

Namen informacijske varnostne politike je [6]:
- varovanje informacij in oseb,
- postaviti pravila pričakovanega obnašanja uporabnikov, sistemskih administratorjev, vodstva in varnostnega osebja,
- pooblastiti varnostno osebje, da lahko spremlja, nadzira in preiskuje,
- definirati posledice kršitev,
- definirati izhodiščno stanje varnosti na nivoju organizacije,
- pomagati zmanjševati tveganje,
- pomagati pri preverjanju skladnosti s predpisi in zakonodajo.

Informacijska varnostna politika prinaša v organizacijo višjo stopnjo varnosti, ki jo doseže samo v primeru sodelovanja službe za informatiko z ostalimi zaposlenimi. Politika sama po sebi ne dvigne stopnje varnosti v organizaciji, ampak jo zaposleni, ki se morajo ravnati v skladu s to politiko. Tako zaposleni zaščitijo informacije in sredstva pred notranjimi in zunanjimi grožnjami. Da se takšno stanje vzdržuje, sta potrebni redna revizija poslovanja in dopolnjevanje politike v skladu z novimi potrebami in grožnjami.

2.1 Zagotavljanja informacijske varnosti

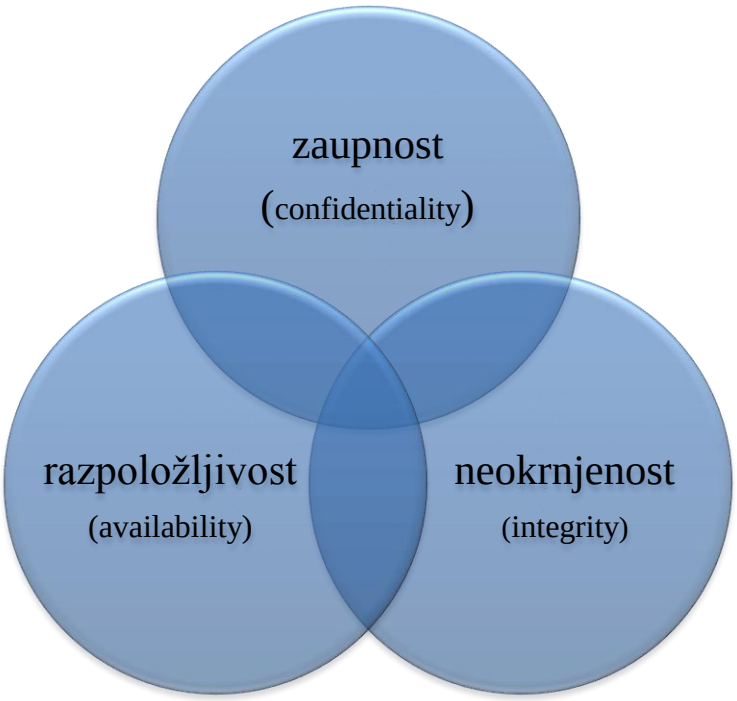
Osnovni cilj informacijske varnosti je zagotavljanje zaupnosti, neokrnjenost, razpoložljivosti IS in njegovih dobrin [23].

Zagotavljanje zaupnosti (angl. confidentiality) pomeni preprečevanje nepooblaščenega razkritja podatkov oz. informacij. Zagotoviti želimo dostopnost podatkov in informacij izključno pooblaščenim osebam.

Zagotavljanje neokrnjenosti (angl. integrity) pomeni preprečevanje nepooblaščenih sprememb v IS. Tako kot zagotavljanje razpoložljivosti se tudi zagotavljanje zaupnosti nanaša na vse dele IS.

Zagotavljanje razpoložljivosti (angl. availability) pomeni zagotavljanje dostopnosti do IS oz. njegovih dobrin v trenutku, ko jih pooblaščeni uporabniki potrebujejo. Zagotavljanje razpoložljivosti se nanaša na vse glavne dele IS: sistemska oprema, programska oprema, podatki/informacije in človek.

Zgornji trije cilji so poznani kot CIA trojček (slika 1) [12].



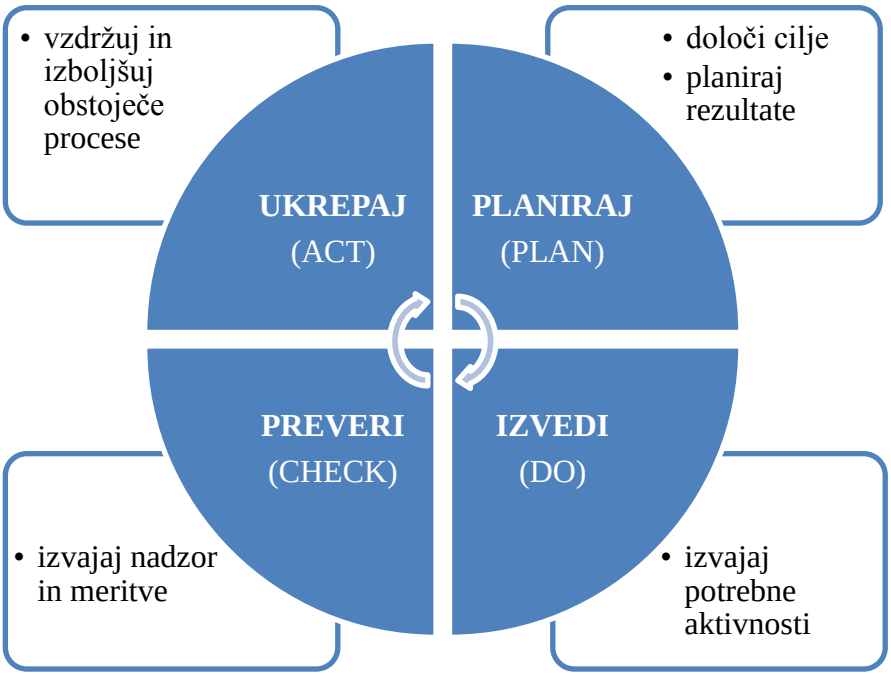
Slika 1: CIA trojček

2.1.1 Sistem upravljanja varovanja informacij

Organizacija, ki želi v svojem okolju vzpostaviti želen nivo informacijske varnosti, mora vzpostaviti ustrezen sistem za upravljanje varovanja informacij (angl. information security management system, krat. ISMS), v nadaljevanju SUVI. SUVI je sistem, ki v organizaciji skrbi za vpeljavo, vzdrževanje in nenehno izboljševanje na področju varovanja informacij. Temeljiti mora na ciljih, ki jih organizacija želi doseči z varovanjem in zaščito, na izbiri

ustrezne strategije, ki bo ustrezala velikosti podjetja, načinu in obsegu poslovanja, sredstvih, organizacijski kulturi ter znanju.

SUVI v organizaciji mora temeljiti na procesnem pristopu PDCA oz. "planiraj – izvedi – preveri – ukrepaj", ki ga uvaja standard ISO/IEC 27001.
Procesni pristop PDCA oz. t.i. Demingov krog je prikazan na sliki 2.



Slika 2: Demingov krog

Osnovo SUVI v organizaciji predstavlja ustrezna dokumentacija. Dokumente, ki z različnih vidikov definirajo SUVI in jih je potrebno v organizaciji izdelati, bi lahko predstavili v obliki piramide [3]. Prikazana je na sliki 3.



Slika 3: Piramida dokumentov, ki definirajo SUVI v organizaciji

Pri zasnovi in vzpostavitvi SUVI si organizacija lahko pomagajo z različnimi standardi, priporočili in primeri dobrih praks. Poleg družine standardov ISO/IEC 27000 so na tem področju na voljo še številni dokumenti. Omeniti velja predvsem največkrat v praksi uporabljene dokumente:

- družina standardov ISO/IEC 27000,
- ITIL: zbirka najboljše prakse za upravljanje informacijskih storitev,
- COBIT: zbirka nadzornih ciljev, ki predstavljajo najboljšo prakso za upravljanje informacijske tehnologije.

V nadaljevanju sledi podrobnejša razlaga posameznih standardov oz. zbirk.

2.2 Standardi družine ISO/IEC 27000

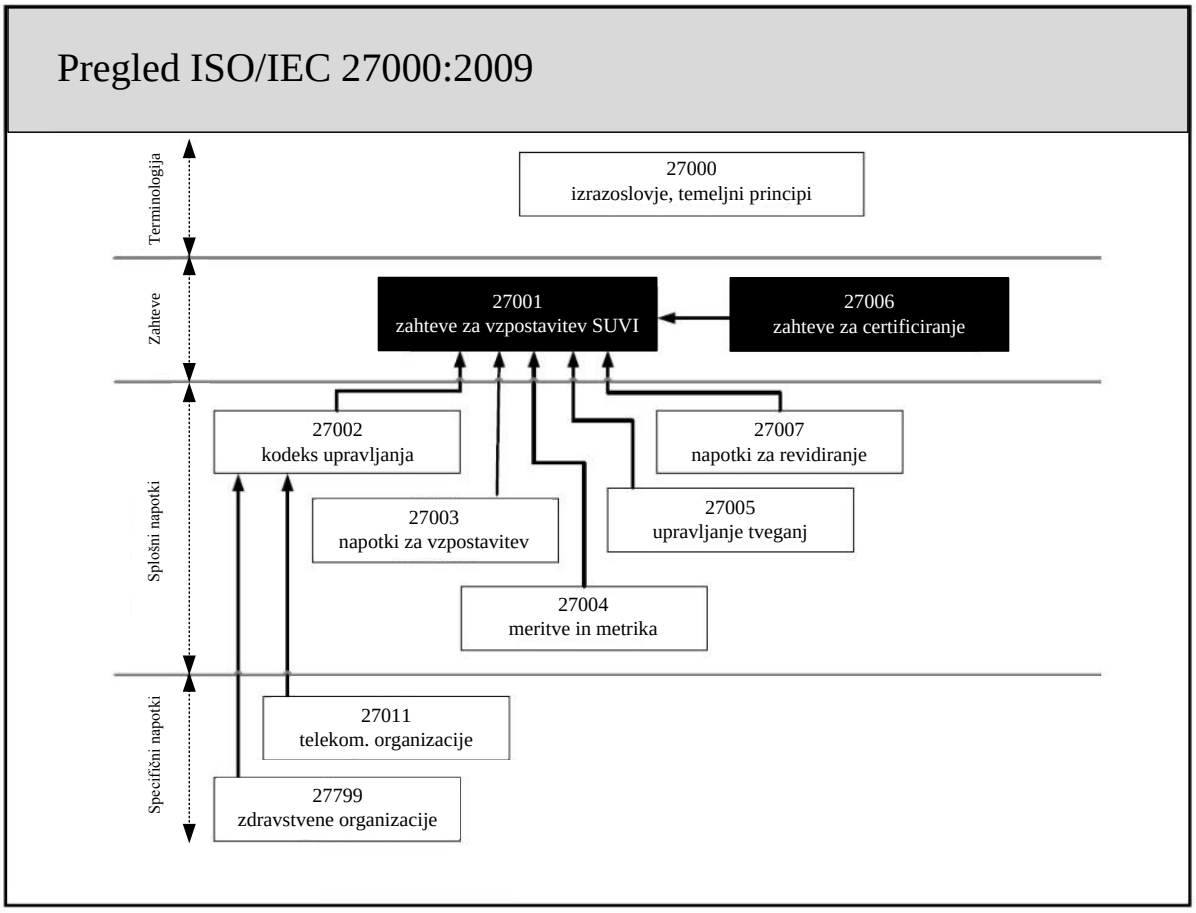
Standardi družine ISO/IEC 27000 so mednarodni standardi za upravljanje informacijske varnosti. Znani so tudi pod imenom ISO27k. Standarde serije ISO objavlja International Organization for Standardization (ISO) v sodelovanju z International Electrotechnical Commission (IEC). Standardi ISO/IEC 27000 vsebujejo priporočila in nasvete za zagotavljanje zaupnosti, neokrnjenosti in razpoložljivosti informacij. Področje uporabe standardov zajema poleg organizacijskega in tehničnega vidika varnosti tudi zasebnost zaposlenih na delovnem mestu. Trenutno je v seriji standardov ISO/IEC 27000 izdanih že preko deset standardov, v prihodnosti pa je predvidenih za izdajo še vsaj 11 standardov [17].

Edini standard po katerem se lahko organizacija certificira, je ISO/IEC 27001. Vsi ostali standardi skupine podajajo dobre prakse za vpeljavo standarda v različna okolja, ter metodologije za vpeljavo. Pri tem je potrebno še poudariti, da standard ISO/IEC 27000 podaja le temeljna načela in definicije za vpeljavo sistema upravljanja varovanja informacij.

Glavni namen informacijskih standardov ISO/IEC 27000 je:

- določitev zahtev za sistem upravljanja varovanja informacij SUVI in presojevalce SUVI,
- zagotovitev neposredne podpore, podrobna navodila in razlage za celoten proces PDCA,
- definicija smernic za posamezne sektorje SUVI,
- opredelitve za ugotavljanje skladnosti SUVI.

Nazornejši pregled standardov družine ISO/IEC 27000 je prikazan na sliki 4.



Slika 4: Pregled standardov ISO/IEC 27000

Za nas sta pomembna ISO/IEC 27001 in 27002, saj nam uporabo narekuje Banka Slovenije skladno z Zakonom o bančništvu (Uradni list RS, št. 83/2004). Ta v tretjem členu zahteva, da mora banka za opravljanje bančnih oz. drugih finančnih storitev upoštevati slovenska standarda SIST BS 7799-2:2003 in SIST ISO/IEC 17799:2003 [18]. Zakon žal ne sledi zadnjim spremembam na tem področju, ampak zahteva upoštevanje varnostnih standardov ISO/IEC 27001:2005 in 27002:2005 oz. SIST ISO/IEC 27001:2010 in SIST ISO/IEC 27002:2008.

Prvi standard določa način uvajanja varnosti v organizaciji, drugi pa je skupek priporočil za zagotavljanje varnega poslovanja.

2.2.1 ISO/IEC 27001

Standard ISO/IEC 27001 je bil izdan oktobra leta 2005 in je zamenjal takratni standard BS7799-2. Podrobno opisuje model SUVI. Standard BS7799 je bil prvič objavljen v devetdesetih letih kot kodeks upravljanja varovanja informacij, kasneje se je pojavil drugi del kot specifikacija z napotki za uporabo.

ISO/IEC 27001 je torej upravljavski standard, ki prevzema procesni pristop PDCA za vzpostavitev, vpeljavo, delovanje, spremljanje, pregledovanje, vzdrževanje in izboljševanje SUVI organizacije [19]. Standard ureja naslednja področja:

- vzpostavitev SUVI (začetek, vpeljava, spremljanje in vzdrževanje, odgovornosti, zahteve kaj je potrebno dokumentirati, kontrole dokumentov, ustreznost dokumentacije, upoštevanje poročil),
- odgovornost vodstva (zaposlenim predstaviti zavezo za uveljavljanje zahtev po varnosti, upravljanje sredstev),
- notranje presoje SUVI (na podlagi spremljanja ugotavljamo uspešnost SUVI),
- vodstveni pregled SUVI (na podlagi poročil, notranje presoje in poslovnih strategij),
- izboljševanje SUVI (preventivni ukrepi v procesu SUVI na podlagi notranjih presoj).

Podrobnejša struktura standarda ISO/IEC 27001 je predstavljena na sliki 5.

0. Uvod		
1. Predmet standarda		
2. Naveza z drugimi standardi		
3. Izrazi in definicije		
4. Sistem vodenja varovanja informacij		
4.1 Splošne zahteve	4.2 Vzpostavitev in delovanje SUVI	4.3 Zahteve glede dokumentacije
5. Odgovornost vodstva		
5.1 Zavezanost vodstva	5.2 Vodenje virov	
6. Notranje presoje SUVI		
7. Vodstveni pregled SUVI		
7.1 Splošno	7.2 Vhodni podatki za pregled	7.3 Rezultat pregleda
8. Izboljševanje SUVI		
8.1 Nenehno izboljševanje	8.2 Korektivni ukrepi	8.3 Preventivni ukrepi
Priloga A	Priloga B	Priloga C

Slika 5: Struktura standarda ISO/IEC 27001:2005

2.2.2 ISO/IEC 27002

Standard ISO/IEC 27002 je kodeks upravljanja varovanja informacij, ki so ga leta 2007 preimenovali iz standarda ISO/IEC 17799. Določa smernice in splošna načela za začetek, izvajanje, vzdrževanje in izboljšanje SUVI v organizaciji. ISO/IEC 27002 predlaga najboljše prakse na področju informacijskih varnostnih ukrepov. Navedeni cilji v tem standardu zagotavljajo splošne smernice za pogosto sprejete cilje vodenja varovanja informacij.

Nadzorni cilji in kontrole v tem standardu so namenjeni temu, da se z njihovo implementacijo izpolni zahteve, ki so bile identificirane z ocenjevanjem tveganj. Standard lahko služi kot praktična smernica za razvoj organizacijskih varnostnih standardov in učinkovite prakse upravljanja varnosti.

Standard ureja naslednjih 12 področij [20]:

- upravljanje s tveganji (analiza tveganj, ocena tveganj, obvladovanje tveganj),
- varnostna politika (politika varovanja informacij),
- organizacija varovanja informacij (infrastruktura varovanja, varovanje dostopa tretje osebe, zunanji viri),
- upravljanje sredstev (odgovornost za sredstva in klasifikacija informacij),
- varovanje človeških virov (varnost pri opredelitvi dela in izbiri sodelavcev, usposabljanje uporabnikov, delo ob incidentih/okvarah),
- fizična zaščita in zaščita okolja (varovana območja, varovanje opreme, druge splošne kontrole),
- upravljanje komunikacij in produkcije (postopki in odgovornosti, načrtovanje in uvajanje, zaščita pred zlonamerno programsko opremo, skrbništvo, upravljanje omrežja, delo z nosilci podatkov, izmenjava programov in informacij),
- nadzor dostopa (upoštevanje poslovnih zahtev, upravljanje dostopov, odgovornosti uporabnikov, nadzor dostopa do omrežja, operacijskih sistemov, aplikacij, spremljanje dostopa in uporabe, prenosna oprema in oddaljeni dostopi),
- nakup, razvoj in vzdrževanje IS (varnostne zahteve, varovanje aplikacij, kriptografija, varovanje sistemskih datotek, varovanje v procesih razvoja in vzdrževanja),
- upravljanje incidentov (zaznava incidenta, reagiranje, reševanje, učenje),
- upravljanje neprekinjenega poslovanja (redni pregledi, kontrole za prepoznavanje in zmanjšanje tveganj),
- združljivost (zakoni, operativni pregledi, notranje presoje IS).

2.3 ITIL

ITIL (angl. IT infrastructure library) je zbirka knjig z opisi in napotki za uvajanje in kakovostno upravljanje IT storitev (angl. IT Service Management), ki temeljijo na uporabi informacijske tehnologije. V ITIL-u je dokumentirana t.i. najboljša praksa za upravljanje IT storitev. Ogrodje je nastalo leta 1980 pri takratni Centralni agenciji za komunikacije in telekomunikacije (CCTA) – sedanji britanski trgovinski urad (OGC). Njeni nastanki segajo v leto 1980. V zgodnjih devetdesetih so mnoge organizacije po Evropi sprejele okvir priporočil ITIL. Odzivi so bili dobri in popularnost je naraščala. V letu 2000 je izšla druga zbirka knjig, ki je bila močno procesno orientirana. Zbirka je vsebovala 7 knjig. Trenutna verzija 3 (ITIL v3) je bila dokončana leta 2007 in je sestavljena iz petih knjig.

Področja, ki jih pokriva tretja izdaja:

- strategija storitev (angl. service strategy),
- načrtovanje storitev (angl. service design),
- prenos storitev v izvedbo (angl. service transition),
- izvajanje storitev (angl. service operation),
- nenehno izboljševanje storitev (angl. continual service improvement).



Slika 6: ITIL v3 življenjski krog storitev

V nadaljevanju sledi nekaj definicij osnovnih pojmov terminologije ITIL, ki so ključni za razumevanje snovi: [1]

- Storitev: sredstvo, ki stranki prinaša določeno uporabno vrednost in je hkrati ne izpostavlja nepredvidljivim stroškom in tveganjem.
- Dogodek: obvestilo, ki zagotavlja informacije o enem ali več upravljanih objektih. Proces, ki se ukvarja z dogodki, se imenuje upravljanje dogodkov.
- Incident: nenačrtovana prekinitev storitve IT ali padec v kakovosti storitve IT. Incident je tudi okvara konfiguracijskega elementa, četudi še ta ni vplivala na delovanje storitev. Proces, ki se ukvarja z incidenti, se imenuje upravljanje incidentov.
- Problem: nepoznan vzrok za pojav enega ali več incidentov. Upravljanje problemov je proces, odgovoren za preprečevanje problemov ter s tem preprečevanje nastanka incidentov, eliminacijo ponovnega pojava incidentov ter zmanjšanje vpliva incidentov, ki se jih ne da preprečiti.

Za naše nadaljnje razumevanje naloge ne potrebujemo razlag celotnega življenskega kroga storitev, temveč se bomo osredotočili le na dva procesa iz področja izvajanja storitev.

Izvajanje storitev

Namen faze izvajanja storitev je uporabnikom in strankam zagotavljati storitve na dogovorjeni ravni (angl. Service Level Agreement, v nadaljevanju SLA) in upravljati z aplikacijami, infrastrukturo in tehnologijo. Šele na tej stopnji življenjskega cikla se pokaže

dodana vrednost poslovanja. Osebje, ki je zadolženo za nemoteno izvajanje storitve mora zagotoviti, da je vrednost dejansko dostavljena.

Glavni procesi izvajanja storitev so:
- upravljanje dogodkov,
- upravljanje incidentov,
- upravljanje z zahtevami,
- upravljanje problemov,
- upravljanje dostopov.

Izvajanje storitev vključuje številne aktivnosti. Za nas so zanimive predvsem naslednje:
- spremljanje in nadzorovanje: da bi zaznali status storitve in konfiguracijskih elementov in na ta način primerno ukrepali (izvedli primerne korektivne akcije),
- upravljanje s konzolo: centralna koordinacijska točka za spremljanje in upravljanje storitev,
- upravljanje z infrastrukturo: hramba, podatkovne baze, posredniška oprema, imeniške storitve, pripomočki, podatkovni centri itd.,
- delovni pogledi na procese iz ostalih stopenj življenjskega cikla: sprememba, konfiguracija, izdaja in razporeditev, razpoložljivost, zmogljivost, znanje, upravljanje s kontinuiteto storitve itd.

Kot smo že napovedali sta v tej fazi za nas pomembna dva procesa: upravljanje dogodkov in upravljanje incidentov.

Upravljanje dogodkov

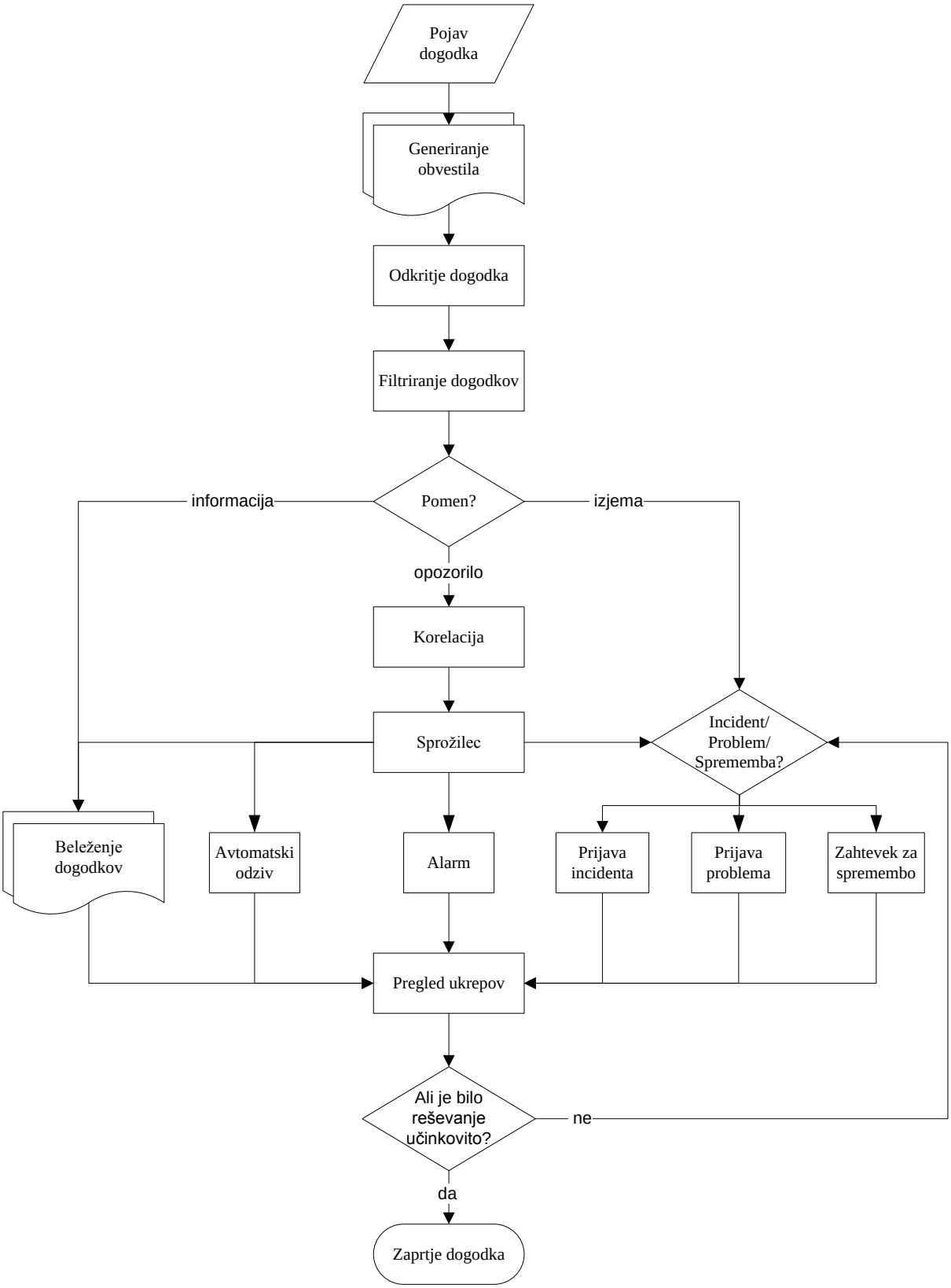
ITIL definira upravljanje dogodkov (angl. event management) kot proces, ki spremlja vse dogodke v IS. V primeru odstopanja od normalnega delovanja pozna procedure obveščanja in eskalacije. Dogodek je definiran kot obvestilo, ki zagotavlja informacije o enem ali več upravljanih objektih [14]. Poleg spremljanja naprav in OS lahko spremljamo tudi varnostne dogodke, uporabo strojne in programske opreme idr. Učinkovito zagotavljanje storitev zahteva, da smo seznanjeni s stanjem storitev. Slednje nam omogoča sistem spremljanja dogodkov, ki zazna morebitne spremembe in nas v najkrajšem možnem času o tem tudi obvesti.

Upravljanje dogodkov ima posreden vpliv na kazalce donosnosti naložbe. V nadaljevanju bomo našteli nekaj takih vplivov.
- S predhodnim alarmom in ustreznim odzivom lahko pravočasno preprečimo morebitno odpoved sistema.
- Z upravljanjem dogodkov prinašamo določeno mero proaktivnosti, saj ne čakamo, da se incident zgodi, temveč imamo možnost reagirati preden nastane operativna škoda.
- Avtomatizem, ki ga pridobimo z upravljanjem dogodkov, pripomore k prerazporeditvi zaposlenih v določenem oddelku oz. le-ti lahko opravljajo druge naloge.
- Omogoča integracijo z ostalimi področji upravljanja storitev, kot so upravljanje incidentov, problemov in sprememb.

Vsaka organizacija ima svojo kategorizacijo dogodkov. ITIL priporoča določitev vsaj treh osnovnih tipov dogodkov:
- Informacija. Odraža normalno delovanje sistema. Npr.: izvoz podatkov je bil uspešno zaključen, uporabnik se je prijavil v aplikacijo, elektronsko sporočilo je bilo uspešno dostavljeno itd.

- Opozorilo. Če je imela informacija zeleno luč na semaforju, ima opozorilo rumeno. Torej delovanje odstopa od običajnega oz. normalnega delovanja. Opozorilo ni razlog za alarm je pa vsekakor potrebno nadaljnje spremljanje storitve. Primer opozorila bi npr. bil, da je prenos podatkov trajal dvajset odstotkov daljši čas kot običajno.
- Izjema. To je tip dogodka na katerega se moramo odzvati. Bodisi gre za grožnjo, kršenje interne varnostne politike, odpovedi strojne opreme itd.

V nadaljevanju si bomo pogledali primer procesa upravljanja dogodkov, ki ga predlaga ITIL (slika 7).



Slika 7: Primer procesa upravljanja dogodkov

Razlaga procesa upravljanja dogodkov.

1. Pojav dogodka. Gre za t.i. rojstvo dogodka. Pomembno je, da zajamemo vse sisteme.
2. Generiranje obvestila. Ko se dogodek pojavi, sistem avtomatsko oblikuje obvestilo.
3. Odkritje dogodka. Ko agent odkrije oz. zazna dogodek, ga posreduje v centralni sistem za upravljanje dogodkov. Pred tem gre dogodek skozi postopek filtriranja.
4. Filtriranje. Na podlagi filtra se določi kateri dogodki bodo šli v nadaljnjo analizo in kateri ne. Filtriranje opravi sistem oz. naprava, ki je generirala dogodek.
5. Kakšen je pomen? Če gre za informacijo, potem se dogodek samo zabeleži. Vsa opozorila gredo v nadaljnjo obravnavo (točka 6). Izjeme pa v preverjanje ali gre za incident, problem ali spremembo.
6. Korelacija. Postopek korelacije je podrobneje opisan v poglavju 3.2.
7. Sprožilec. Rezultat korelacije je običajno nek odziv. Sprožilec je mehanizem, ki sproži ta odziv. Bodisi sproži nov incident, alarm, požene program idr.
8. Odziv. Nekaj odzivov smo že našteli, obstaja jih še mnogo drugih. ITIL priporoča definiranje vsaj osnovnih šest odzivov:
   - beleženje dogodkov,
   - avtomatski odziv,
   - alarm, pri katerem je potrebno človeško posredovanje,
   - zahtevek za spremembo (zahtevek je posredovan sistemu za upravljanje s spremembami),
   - prijava incidenta (zahtevek je posredovan sistemu za upravljanje z incidenti, običajno je to storitveni center),
   - prijava problema (zahtevek je posredovan sistemu za upravljanje s problemi, običajno je to storitveni center).
9. Pregled ukrepov (ali je bilo reševanje učinkovito). Utopično bi bilo pregledati vse dogodke. Zadostuje, če se osredotočimo na bolj pomembne dogodke in izjeme. Dogodek lahko zaključimo, če so bili ukrepi zadostni. V nasprotnem primeru gre dogodek v ponovno obravnavo.
10. Zaprtje dogodka. Dogodek, ki se samo zabeleži, lahko takoj zaključimo. Dogodki, ki so vezani na generiranje nove spremembe/incidenta/problema pa se zaključijo šele, ko so ti zaključeni.

Upravljanje incidentov

ITIL definira upravljanje incidentov (angl. incident management) kot celovit proces upravljanja nepričakovanih dogodkov. Incident je definiran kot nenačrtovana prekinitev izvajanja storitve ali zmanjšanje njene kakovosti. Prav tako je incident napaka na konfiguracijskem elementu, četudi ta napaka še ni vplivala na samo storitev [14].

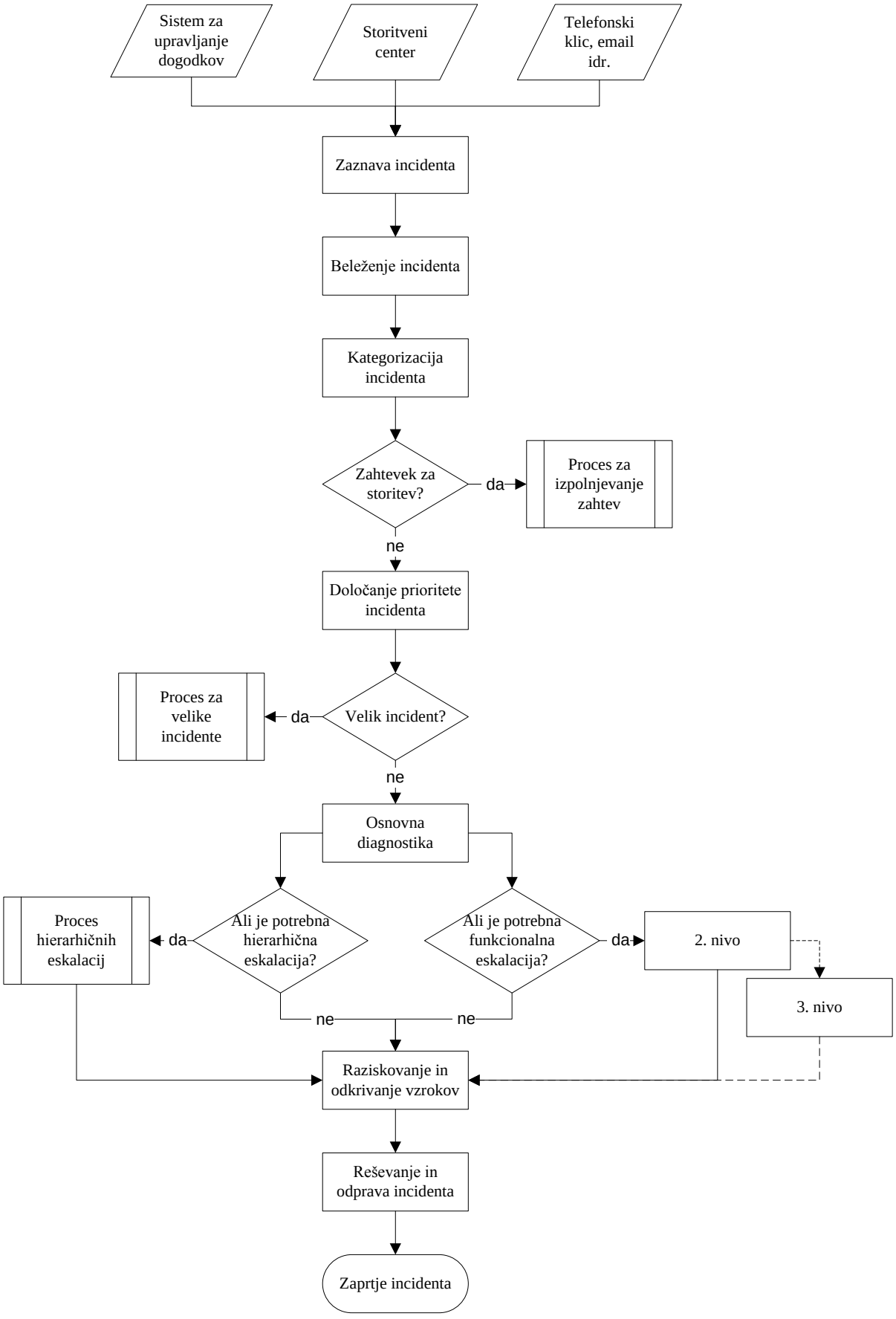
Cilj upravljanja incidentov pomeni kar se da hitro vzpostavitev normalnega stanja delovanja storitev, kar sproži minimiziranje negativnih vplivov na poslovanje. Upravljanje incidentov se navezuje na vsak dogodek, ki negativno vpliva ali bi lahko v prihodnosti negativno vplival na storitev. Torej tu so zajeti vsi dogodki, ki jih posreduje sistem za upravljanje dogodkov in tisti, ki jih uporabniki oddajo preko storitvenega centra (angl. service desk). Pri avtomatskem generiranju dogodkov je potrebno biti pazljiv, saj niso vsi dogodki incidenti, ampak so nekateri lahko le informacijske narave. Upravljanje incidentov je za organizacijo poglaviten proces, ki zagotavlja nemoteno delovanje ostalih storitev. Njegova neposredna povezanost s poslovanjem je še razlog več, da se vodstvo odloči podpreti projekt postavitve storitvenega centra. Zato je storitveni center pogosto ena prvih funkcij, ki se jo vpelje v sklopu upravljanja storitev v IT. Implementacija storitvenega centra ni predmet te naloge, saj je bilo na to temo

že veliko napisanega [16]. Za nadaljnjo razpravo je pomembno dejstvo, da je storitveni center glavni pogoj za uspešno upravljanje incidentov.

Pri osnovni vzpostavitvi procesa upravljanja incidentov je potrebno upoštevati tri pomembne dejavnike.

- Določiti je potrebno časovne okvire za posamezne stopnje obravnavanja incidentov. Te določitve so del krovnega SLA, ki ga sestavljajo dogovori o ravneh izvajanja (angl. operational level agreement) in pogodbe z zunanjim ponudniki storitev (angl. underpinning contract). Vse podporne skupine morajo poznati te časovne okvire in jih tudi upoštevati.
- Večje število sprejetih incidentov je že znanih oz. so se le-ti že pojavili. To je eden izmed razlogov, da ITIL priporoča definiranje t.i. modela za upravljanje incidentov. S tem pristopom lahko vse incidente obravnavamo po vnaprej določenih korakih ter v predvidenem časovnem obsegu. Model za upravljanje incidentov predstavlja vnaprej določene korake, ki se izvedejo pri rokovanju z incidenti. Tak model naj bi vseboval korake, ki so potrebni za rešitev incidenta, kronološko zaporedje teh korakov, odgovornosti, aktivnosti za funkcionalno eskalacijo ter časovne okvire za razrešitev incidenta.
- Za vse velike oz. pomembne incidente je potrebno vzpostaviti ločene procedure s krajšim rokom razrešitve incidenta. Hkrati imajo taki tipi incidentov tudi višjo prioriteto, kar pomeni, da imajo prednost pred ostalimi. Pri tem je potrebno najprej definirati kateri incidenti sploh spadajo v kategorijo velikih incidentov. Nato se tej skupini incidentov določi prioriteto, ki je v skladu z internimi pravili. V primeru da ima velik incident poznano rešitev, ocenjujemo, da bo odpravljen v dogovorjenem roku. Zato ni potrebno, da bi incident razreševali po ločeni proceduri. V takem primeru se poraja vprašanje zakaj prihaja do ponovljivih velikih incidentov. S tem področjem se podrobneje ukvarja proces upravljanja problemov (angl. problem management).

V nadaljevanju si bomo pogledali primer procesa upravljanja incidentov, ki ga predlaga ITIL (slika 8).



Slika 8: Primer procesa upravljanja incidentov

Razlaga procesa upravljanja incidentov.

1. Zaznava incidenta. Brez zaznave incidenta ni mogoče sprožiti nadaljnjih postopkov. Zaznava incidenta je mogoča na več načinov: incident nam lahko posreduje sistem za upravljanje dogodkov preko storitvenega centra, telefonskega klica itd.
2. Beleženje incidenta. Pomembno je, da se vsi incidenti zabeležijo. Pri beleženju skušamo zbrati čim več informacij povezanih z incidentom: čas nastanka incidenta, kateri sistem, kakšen je vpliv na sistem in ostale sisteme, prioriteta idr.
3. Kategorizacija. Incident je potrebno pravilno kategorizirati. Najnižji nivo kamor lahko kategoriziramo incident je konfiguracijski element. Pri tem pa je prej potrebno vzpostaviti ustrezno hierarhijo kategorij. Primer nedelujočega napajalnika bi sodil v naslednjo kategorijo: strojna oprema → strežnik →HP DL380G5 →napajalnik
4. Ali je zahtevek za storitev? V primeru zahtevka za storitev se sproži standarden postopek za izpolnjevanje zahtev (angl. request fulfilment).
5. Določanje prioritete incidenta. Pri določanju prioritete je potrebno upoštevati kakšen učinek ima incident in s kakšno nujnostjo je potrebno incident razrešiti. Obstaja več metod za določanje prioritet [22].
6. Ali je velik incident? Če gre za velik incident potem ga obravnavamo prioritetno in uporabimo predpisano ločeno proceduro.
7. Osnovna diagnostika. Osnovno diagnostiko opravi prva stopnja podpore, ki tudi poskuša prva razrešiti incident.
8. Ali je potrebna funkcionalna eskalacija? Prva stopnja podpore presodi ali je potrebna funkcionalna ali hierarhična eskalacija.
9. Raziskovanje in odkrivanje vzrokov. Pri odkrivanju vzroka se uporabi vse informacije zbrane skozi celoten proces. Pomisliti je potrebno na kaj vse lahko vpliva dani incident in kakšne posledice bo imel.
10. Reševanje in odprava incidenta. Ko je rešitev znana, jo posredujemo pristojnim v izvedbo. Bodisi je to tehnična podpora, sistemski administrator ali zunanji izvajalec.
11. Zaprtje incidenta. Ko dobi prva stopnja podpore povratno informacijo, da je incident odpravljen, se lahko zaključi incident.

Vloge oseb na področju upravljanja incidentov so sledeče:

- Upravitelj incidentov je lastnik procesa upravljanja incidentov in se velikokrat pojavlja tudi v vlogi upravitelja storitvenega centra, kar pa ni nujno.
- Prva stopnja podpore ima tri osnovne naloge: beleženje incidentov, opravljanje osnovne diagnostike ter reševanje najenostavnejših incidentov. Velika večina incidentov se reši znotraj storitvenega centra.
- Druga stopnja podpore zahteva večjo stopnjo znanja in specializacije. Incident je dodeljen v reševanje v primeru funkcionalne eskalacije iz prve stopnje. Zaključitev incidenta opravi prva stopnja.
- Tretja stopnja podpore izvaja reševanje tehnično najzahtevnejših incidentov. To delo opravljajo strokovnjaki, ki imajo širok spekter znanja in dobro poznavanje IS. V primeru da posameznik ni zmožen sam odpraviti incidenta, prosi za pomoč širšo skupino strokovnjakov. V nekaterih primerih se lahko v reševanje incidenta vključi tudi pomoč zunanjega partnerja oz. svetovalca. Incident je dodeljen v reševanje v primeru funkcionalne eskalacije iz prve ali druge stopnje. Tudi tu zaključitev incidenta opravi prva stopnja.

2.4 COBIT

Prva različica COBIT-a je bila definirana leta 1996 s strani neprofitne organizacije ISACA in ITGI. Danes je v širši uporabi različica 4.1, ki je zasnovana na ustaljenih okvirih kot so: CMM, ISO9000, ITIL in ISO/IEC 27002. Gre za mednarodno sprejet okvir za kontrolo upravljanja IT, ki predstavlja aktivnosti na obvladljiv in logičen način. Okvir COBIT je bil oblikovan tako, da njegove glavne značilnosti kot je osredotočenost na poslovanje in usmerjenost na procese temeljijo na kontrolah in so vodene z meritvami. COBIT se osredotoča bolj na kontrolo in manj na izvajanje. Običajno je ciljna publika vrh uprave oz. IT vodstvo ter presojevalci in revizorji.

Osredotočenost na poslovanje
Osredotočenost na poslovanje je glavna tema COBIT-a. Po obliki ni namenjen le uporabi s strani izvajalcev storitev IT, uporabnikov, revizorjev in presojevalcev, temveč zagotavlja tudi obsežna navodila vodstvu in lastnikom poslovnih procesov.

Okvir COBIT temelji na načelu zagotavljanja informacij.
Za zagotovitev informacij, ki jih podjetje potrebuje za uresničitev svojih ciljev, mora vlagati, upravljati in nadzorovati vire IT z uporabo strukturiranega sklopa procesov. S tem zagotovi storitve, ki dajejo informacije [8].

Usmerjenost na procese
COBIT opredeljuje dejavnosti IT v okviru splošnega procesnega modela znotraj štirih domen. Domene začrtajo tradicionalna področja zadolžitev v zvezi z IT, in sicer: načrtujte, vzpostavite, izvajajte in spremljajte.

Okvir COBIT vsebuje 4 domene, 34 procesov in 210 kontrolnih ciljev:
- Načrtujte in organizirajte (PO, angl. Plan and Organise) - zagotavlja usmeritev k iskanju rešitve (AI) in izvajanju storitev (DS).
- Nabavite in vpeljite (AI, angl. Acquire and Implement) - zagotavlja rešitve in jih posreduje, da se pretvorijo v storitve.
- Izvajajte in podpirajte (DS, angl. Delivery and Support) - sprejema rešitve in poskrbi, da so uporabne za končne uporabnike.
- Spremljajte in vrednotite (ME, angl. Monitor and Evaluate) - spremlja vse procese za zagotovitev, da se upošteva določena usmeritev.

Temelji na kontrolah
COBIT opredeli kontrolne cilje za vseh 34 procesov ter splošne procesne in aplikativne kontrole.
Kontrolni cilji IT zagotavljajo popoln nabor zahtev na visoki ravni, ki jih mora upoštevati vodstvo za uspešen nadzor vsakega procesa IT. Kontrolni cilji so:
- izjave o ukrepih vodstva za povečanje vrednosti ali zmanjšanje tveganja,
- sestavljeni iz politik, postopkov, praks in organizacijske strukture,
- oblikovani tako, da zagotovljajo razumno jamstvo, da bodo poslovni cilji doseženi ter neželeni dogodki preprečeni ali odkriti in popravljeni.

Poleg kontrolnih ciljev ima vsak COBIT-ov proces splošne kontrolne zahteve, ki so opredeljene z oznako PCn, tj. številka kontrole procesa (angl. Process Control number):
- PC1 Cilji procesa,
- PC2 Lastništvo procesa,

- PC3 Ponovljivost procesa,
- PC4 Vloge in zadolžitve,
- PC5 Politika, načrti in postopki,
- PC6 Izboljšanje zmogljivosti procesa.

Naslednji seznam zagotavlja priporočen nabor aplikacijskih kontrolnih ciljev. Označeni so kot ACn, kjer je n številka aplikacijske kontrole (angl. Application Control number):

- AC1 priprava in odobritev izvornih podatkov,
- AC2 zbiranje in vnos izvornih podatkov,
- AC3 preverjanje pravilnosti, popolnosti in verodostojnosti,
- AC4 veljavnost in celovitost obdelave,
- AC5 pregled in uskladitev rezultatov ter odprava napak,
- AC6 overjanje in celovitost transakcije.

Voden z meritvami

Osnovna potreba vsakega podjetja je pridobiti razumevanje stanja IS in se odločiti kakšno raven upravljanja in kontrole mora zanje zagotoviti. Pridobivanje objektivnega vpogleda v lastne ravni zmogljivosti podjetja ni preprosto. Podjetja morajo meriti kakšno je njihovo stanje in katere izboljšave so potrebne. Poleg tega morajo vpeljati orodja za upravljanje spremljanja izboljšanja. COBIT obravnava ta področja z zagotovitvijo:

- zrelostnih modelov, ki omogočajo primerjalno analizo in prepoznavanje potrebnih izboljšav zmožnosti,
- ciljev izvedbe in metrik za procese IT, ki kažejo kako procesi uresničujejo poslovne cilje in cilje IT,
- ciljev dejavnosti za omogočanje uspešne izvedbe procesov.

3. Upravljanje varnostnih informacij in dogodkov

3.1 Osnovni pojmi

Prvotno so bili dnevniki namenjeni le za osnovno beleženje dogajanja na omrežnih in drugih napravah. Danes pa imajo bistveno večji pomen. Njihove informacije izkoriščamo pri: optimizaciji sistemov, izboljšanju performanc omrežja, spremljanju uporabniških aktivnosti, ugotavljanju varnostnih kršitev, zagotavljanju skladnost s standardi oz. predpisi itd. Ta široka uporabnost dnevnikov je bila povod za nastanek nove veje, ki se ukvarja z upravljanjem dnevnikov (angl. log management).

V začetku 90-ih je bil izvor dnevnikov zelo ozek in večino domena omrežnih naprav (usmerjevalniki, preklopniki idr.). Temu danes ni več tako, saj je izvor dnevnikov izredno širok. Poleg omrežnih naprav dnevnike generirajo še strežniki sistemi, delovne postaje, aplikacije, operacijski sistemi, podatkovne baze, pametni telefoni in druge naprave. To je ustvarilo potrebo po centraliziranem upravljanju dnevnikov.

Podjetja, ki so se odločila za postavitev takega sistema, so kmalu uvidela pravi potencial te rešitve. Poleg poenostavljenega iskanja dogodkov je sistem omogočal izvajanje analiz in poročil o skladnosti. To področje se imenuje upravljanje varnostnih informacij (angl. Security Information Management). Prvi standard na temo upravljanja dnevnikov je bil izdelan šele leta 2006. Izdala ga je organizacija NIST: "Guide to Computer Security Log Management (NIST SP800-92)".

Razvoj je šel dalje in v obstoječi sistem so dodali dodatne funkcije za upravljanje z dnevniki. Največja pridobitev je bila funkcionalnost, ki omogoča spremljanje dogajanja v realnem času. Spremljanje dogajanja vključuje spremljavo vseh vitalnih delov IS, to pomeni: naprav, aplikacij in uporabnikov. To področje se imenuje upravljanje varnostnih informacij in dogodkov (angl. Security Information and Event Management).
Kratica SIEM se je prvič pojavila leta 2003 pri podjetju Gartner. Gre za vsebinsko združitev dveh uveljavljenih varnostnih področij:

1. Upravljanje varnostnih informacij (angl. Security Information Management, krat. SIM).
2. Upravljanje varnostnih dogodkov (angl. Security Event Management, krat. SEM).

Od tod tudi izvor kratice SIEM:

$$SIM + SEM = SIEM$$

Pred nadaljevanjem je potrebno razjasniti izrazoslovje na tem področju.
Dogodek (angl. event) je zaznana aktivnost, pripetljaj ali sprememba stanja. Vsak dogodek vsebuje določene informacije o dogodku, ki so zabeležene v poljih.

Kategorija (angl. category) opredeljuje izvor dogodka. Poznamo naslednje kategorije: varnostna, aplikacijska, sistemska idr.

Polje v dogodku (angl. event field) vsebuje določeno informacijo o dogodku. Primer takega polja je npr.: datum, ura, izvorni naslov, prioriteta, opis idr.

Dnevniški zapis (angl. event record) predstavlja skupek oz. množico polj, ki opisujejo dogodek. V angleščini obstajata še dva sinonima za event record. To sta audit record in log entry.

Dnevnik (angl. log) je zbirka dnevniških zapisov. Drugi sinonim je dnevnik dogodkov (angl. event log). V nalogi bomo uporabljali izraz dnevnik. Dnevniki bodo naš primarni vir informacij in z njimi povezani dogodki. Poznamo več vrst dnevnikov, ki jih ločimo glede na njihov izvor:

- varnostni dnevnik (angl. security log),
- sistemski dnevnik (angl. system log),
- aplikacijski dnevnik (angl. application log),
- bazni dnevnik (angl. database log) idr.

Dnevniška datoteka (angl. log file) je datoteka, kjer se shranjuje dnevnik oz. njegovi dnevniški zapisi. Podobno kot dnevnik se tudi dnevniške datoteke ločijo glede na njihov izvor. Besedno zvezo dnevniška datoteka bomo uporabili v primeru, ko bomo želeli poudariti, da gre za prenos oz. transport dnevnika. V vseh drugih primerih pa bomo uporabili skupen izraz – dnevnik.



Slika 9: Relacije med izrazi

3.2 Upravljanje varnostnih informacij

Začetki področja upravljanja varnostnih informacij (v nadaljevanju SIM) segajo v leto 1990. Takrat se je pojavila potreba po zbiranju dnevniških datotek iz omrežnih naprav. Delovanje takih aplikacij je bilo sila preprosto. Zajem dnevniških datotek se je izvajal s pull metodo (glej poglavje 4.2). V aplikaciji je bilo omogočeno le pregledovanje dnevnikov brez dodatne logike. S časom so SIM aplikacije pridobivale nove funkcionalnosti. Zajem dnevniških datotek se je tako iz omrežnih naprav, razširil še na OS in aplikacije. Prvotni namen SIM aplikacij je predstavljal ureditev centralne zbirke dnevnikov, ki je nadalje omogočala izvajanje raznih analiz in izdelavo poročil.

Rezultati raziskav organizacije SANS [34] kažejo, da je eden glavnih razlogov zakaj se podjetja odločajo za postavitev SIM sistema, potreba po zagotavljanju skladnosti. Podjetja so ugotovila, da je kršenje skladnosti dražje kot nakup sistema SIM (SIEM). V takem primeru je nakup upravičen, bodisi gre za zagotavljanje skladnosti po določenem standardu (ISO/IEC 27001, Basel II, PCI DSS, SOX, GLBA, HIPAA idr.) ali za ugotavljanje kršitev interne varnostne politike.

3.3 Upravljanje varnostnih dogodkov

Leta 1999 se je v svetu informacijske varnosti pojavilo novo področje, ki se je začelo ukvarjati z upravljanjem varnostnih dogodkov (v nadaljevanju SEM). SEM sistem si lahko

predstavljamo kot nekakšen procesni center za dnevniške datoteke in varnostne dogodke. Slednje zajema iz omrežnih naprav, operacijskih sistemov in aplikacij. S pomočjo vgrajene logike, ki omogoča vrsto naprednih funkcij za delo z dnevniškimi datotekami, nam sistem omogoča še lažje odkrivanje notranjih in zunanjih varnostnih kršitev. Glavna prednost SEM sistemov je, da omogočajo spremljanje dogajanja v realnem času. Slednje pa pripomore k boljšem pregledu stanja nad IS, ter zmanjšanju reakcijskega časa v primeru incidenta.

3.4 Upravljanje varnostnih informacij in dogodkov

Področji SIM in SEM sta se zaradi vse večjega medsebojnega povezovanja in prepletanja funkcionalnosti združili pod enotno področje, ki se imenuje upravljanje varnostnih informacij in dogodkov (angl. Security Information and Event Management). V nadaljevanju naloge bomo uporabljali skupen izraz za to področje – SIEM.

Sistemi SIEM vsebujejo funkcionalnosti iz obeh področij (SIM in SEM). Omogočajo zajem in hrambo varnostnih dogodkov kot tudi njihovo analizo v realnem času. Bistveno večji poudarek je na spremljanju in nadzoru IS. Šele ko v nadzor zajamemo celotno informacijsko infrastrukturo in uporabnike, dobimo pregled nad celotnim dogajanjem. S tega vidika bi lahko SIEM primerjali s komandnim stolpom [11].

Sledi podroben pregled celotnega nabora funkcionalnosti sistemov SIEM [28, 30].

Upravljanje dnevnikov in poročanje
Je ena izmed osnovnih funkcionalnosti vsakega sistema SIEM. Brez te funkcije si ne moremo predstavljati pravega sistema SIEM oz. je tak sistem pogojno uporaben. Komponenta skrbi za zajem, prenos in shranjevanje dnevniških datotek in drugih varnostnih dogodkov iz zalednih sistemov in naprav. Nudi možnost indeksiranja in šifriranja podatkov. Poleg tega je pomembno, da ima vgrajeno funkcijo iskanja in izdelave poročil.

Normalizacija dogodkov
Normalizacija je postopek poenotenja vseh dnevnikov v skupen format (glej poglavje 4.2). Brez tega postopka bi bila nadaljnja analiza dogodkov otežena in zamudna. Podrobnejša razlaga formatov sledi v poglavju 4.3.

Spremljanje v realnem času
IS lahko dnevno ustvari nekaj milijonov dogodkov in če jih želimo analizirati, potrebujemo ustrezno logiko. Brez normalizacije in korelacije dogodkov bi bil postopek analize v realnem času nemogoč. Korelacija se izvede po postopku normalizacije in omogoča korelacijo med obstoječimi pravili. Glede na vzpostavljeno politiko korelacij med različnimi dogodki se prožijo alarmi v realnem času, ki omogočajo pravočasno zaznavanje varnostnih incidentov, anomalij in nepravilnosti v delovanju IS. Zaželeno je, da sistem vsebuje že predpripravljena korelacijska pravila, katera je mogoče še dodatno prilagoditi lastnim potrebam.

Nadzorna plošča
Vizualni del sistema SIEM predstavlja t.i. nadzorna ali pregledna plošča (angl. dashboard). Gre za grafični vmesnik, ki omogoča spremljavo dogajanja v realnem času (angl. real-time monitoring). Na nadzorni plošči je v obliki grafov in tabel predstavljeno trenutno stanje sistema. Pogostokrat vključuje tudi vpogled v ključne kazalnike uspeha (angl. key performance indicator, krat. KPI).

Podpora za upravljanje incidentov
V primeru zaznanih incidentov potrebujemo ustrezno podporo za njihovo obravnavo. Zato so proizvajalci vgradili podporo za upravljanje incidentov (angl. incident management) v obliki delovnih tokov. Če sistem SIEM nima vgrajene omenjene podpore, je priporočljivo, da vsebuje komponento, ki omogoča nadaljnjo povezljivost oz. integracijo s centralnim sistemom za upravljanje incidentov.

Spremljanje podatkov
Spremljanje podatkov (angl. data monitoring) je široko področje. V kontekstu sistemov SIEM bomo obravnavali naslednje tri sklope:

a) Nadzor sistema za upravljanje podatkovnih baz (angl. database management systems, krat. DBMS)
SIEM nam omogoča tri načine nadzora nad dogajanjem v podatkovni bazi (v nadaljevanju PB):
   - preko dnevniških datotek,
   - z vgrajeno funkcionalnostjo DAM (angl. database activity monitoring),
   - s povezavo do zunanjega sistema DAM.

   Nadzor PB preko dnevniški datotek nam nudi le osnovne informacije. Veliko več možnosti nam nudi funkcionalnost DAM. To je sistem, ki zajema in beleži dogodke, ki se zgodijo na PB. Sem sodijo vse transakcije, nadzor uporabniških aktivnosti na bazi, nadzor privilegiranih računov (baznih administratorjev, angl. database administrators) idr. Po načinu delovanja DAM zelo spominja na SIEM. Oba zbirata in analizirata podatke. Oba zajemata podatke iz različnih virov/baz, kar pomeni, da je pred analizo podatkov potrebna normalizacija in korelacija. Oba poročata in alarmirata v primeru zaznane zlorabe. Razlika je le v vsebini: DMA je specializiran za PB, SIEM pa za vse ostale naprave. Ampak tudi ta razlika počasi bledi, saj se vse več proizvajalcev trudi vključiti funkcionalnost DAM v SIEM. Podjetje TriGeo je v svoj glavni produkt (TriGeo Security Information Manager) že vgradilo DAM.

b) Sistem za nadzor integritete datotek (angl. file integrity monitoring, krat. FIM)
   Kot že ime pove gre za odkrivanje sprememb na nivoju datotek (podatkovne datoteke, programske datoteke, sistemske datoteke, knjižnice idr.). FIM deluje tako, da vsakič, ko se datoteka spremeni, primerja prejšnjo vsebino z novo. V primeru odstopanja sproži alarm. Seznam preverbe je določen s politiko. Ta je lahko zelo ohlapna ali pa zelo stroga. Potrebno je najti nek kompromis, saj nobena od skrajnosti ne prinaša koristi. Pri preohlapni politiki se nam lahko zgodi varnostni incident za katerega sploh ne bomo opozorjeni. Druga skrajnost pa je, da želimo nadzorovati vse datoteke ne glede na njihovo pomembnost. Ta primer pa lahko vodi do preobremenjenosti sistema in posledično do zaustavitve.

   V izogib omenjenim raziskovalno podjetje Securosis predlaga naslednje tri ukrepe [28]:
   1. Nadzor omejimo samo nad pomembnimi datotekami (datoteke z zaupno vsebino, kritične sistemske in operacijske datoteke).
   2. Postavimo prioritetno listo, ki jo vključimo v nadzorno politiko. Na vrh prioritetne liste postavimo znane napade na ključne sisteme.
   3. Za razbremenitev administratorjev, znižamo prioriteto pregledovanja odobrenih sprememb.

c) Sistem za preprečevanje izgube podatkov (angl. data loss prevention, krat. DLP)
DLP je vedno bolj aktualno področje informacijske varnosti. Sistem je lahko del programske opreme ali pa namenska naprava (angl. appliance). Ker gre za kompleksen sistem, se ta ne vgrajuje v SIEM, ampak se sistema povežeta s povezovalno komponento. Na ta način nam SIEM omogoča zajem podatkov. DLP je pomembno orodje za zagotavljanje skladnosti in ugotavljanje notranjih groženj, kot je npr. odtekanje podatkov. Podjetji Symantec in RSA sta edina proizvajalca, ki hkrati ponujata SIEM in DLP rešitev. Oba omogočata povezavo do McAfee DLP 9, vodilnega DLP sistema v letu 2010.

Spremljanje uporabnikov
SIEM omogoča spremljanje uporabniških aktivnosti (angl. user activity monitoring, v nadaljevanju UAM) na več nivojih. Pred tem si mora SIEM zgraditi bazo uporabnikov s pripadajočimi mehkimi informacijami (seznam aplikacij, ki jih uporablja oz. seznam privilegijev do uporabe aplikacij, dostop do podatkovne baze, dostop do skupnih virov itd.). To stori s pomočjo povezave na različne sisteme: Microsoftov aktivni imenik (angl. active directory, krat. AD), sistem za upravljanje identitet (angl. identity management, krat. IdM) idr.

Pred vzpostavitvijo UAM moramo odgovoriti na naslednja tri vprašanja:

1. Kaj predstavlja uporabnika?
   Poleg uporabniškega računa so tu še servisni računi in računalniški računi. Pri izgradnji baze uporabnikov oz. računom nas zanimajo naslednji tipi informacij: uporabniško ime, kje je račun definiran, članstvo skupin, lastnosti (lokacija, telefon, nadrejeni itd.), način avtentikacije, življenjski cikel računa idr.
2. Katere aktivnosti bomo beležili?
   Priporočljivo je beležiti naslednje aktivnosti: sistemske aktivnosti, aktivnosti na podatkovni bazi, aplikacijske aktivnosti, aktivnosti povezane s spremembo strojne in programske opreme idr.
3. Katere so tipične aktivnosti za določeno skupino uporabnikov?
   Pripraviti je potrebno sezname aktivnosti za določene skupine uporabnikov ter ustrezne politike.

Najbolj enostaven primer spremljanja identitet je poročilo o uporabniških prijavah in odjavah v računalnik. Vendar UAM zmore veliko več, npr.: nadzor privilegiranih uporabniških računov (ti. administratorski računi), poročanje v primeru zlorabe pooblastil idr.

Spremljanje aplikacij
Spremljanje aplikacij (angl. application monitoring, v nadaljevanju AM) omogoča povezavo z drugimi aplikacijami. Namen je zajeti želene podatke iz drugih aplikacij v SIEM ter na ta način še dodatno razširiti celotno sliko dogajanja v IS. Za efektivno spremljanje aplikacij je potrebno AM modulu omogočiti dostop do aplikacije, podatkov in uporabniškega nivoja (tj. nivo kjer aplikacija izvaja avtentikacijo oz. avtorizacijo). Naslednji korak je nastavitev AM modula. Ta obsega štiri glavne nastavitve:

- integracija z aplikacijo,
- zajem podatkov,
- določitev formata podatkov,
- prenos podatkov (izmenjava podatkov med AM in SIEM mora biti šifrirana).

V zadnjih desetih letih opažamo velike premike na tem področju. Izdelovalci programske opreme se zavedajo varnostnih tveganj, zato so začeli v svoje aplikacije vgrajevati varnostne mehanizme [7].

AM integracija je najbolj pogosta v kombinaciji z naslednjimi aplikacijami:
- spletni strežnik (Apache, Microsoft IIS, nginx, GWS idr.),
- poštni strežnik (Microsoft Exchange Server, IBM Lotus Domino idr.),
- širok nabor aplikacij iz področja ERP in HR (SAP, Oracle, Microsoft idr.).

Namestitev in podpora

Sistemi SIEM so prilagodljivi in tako dostopni tudi manjšim organizacijam z omejenimi finančnimi viri in človeškimi resursi. Manjše organizacije se odločajo za implementacijo omejenega nabora SIEM funkcionalnosti. Običajno je v tem segmentu največ zanimanja za dokazovanje skladnosti in izdelavo poročil. Proizvajalci ponujajo različne namestitvene pakete z možnostjo podpore pri začetni postavitvi sistema. Sam proces postavitve lahko traja od nekaj mesecev pa tudi do več let. Podrobnosti o namestitvi sistema SIEM so v poglavju 5.5.

4. Opis delovanja sistema SIEM

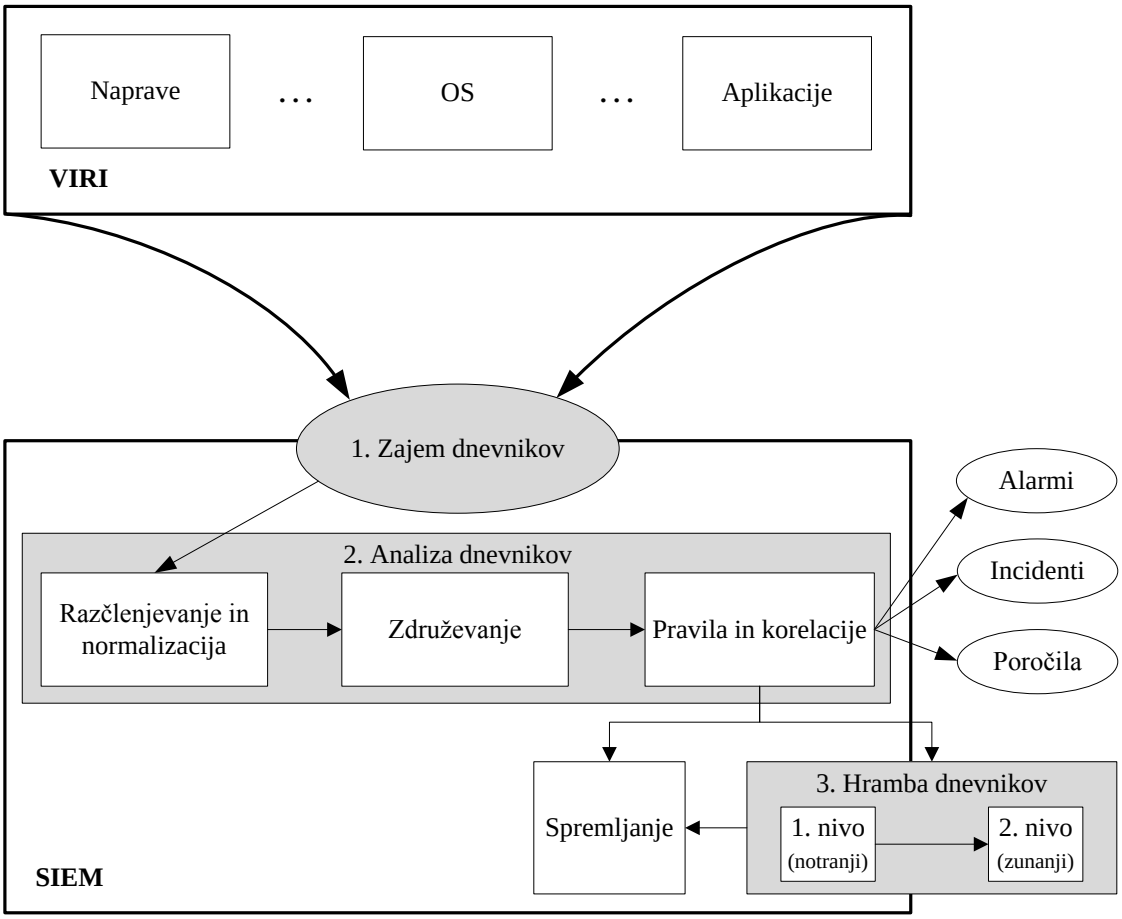
4.1 Splošno

Med SIEM proizvajalci obstajajo različne interpretacije delovanja njihovega sistema. Obstajajo določene skupne značilnosti v delovanju, ki veljajo za vse sisteme SIEM. V splošnem opravlja vsak sistem SIEM tri glavne naloge:

1. Zajem dnevnikov
   To je primarna naloga vsakega sistema SIEM. Zajeti dnevniki in dogodki so vhodni podatki za sistem SIEM in predpogoj za nadaljnjo analizo. Za zajem dnevnikov se v splošnem uporabljata dve metodi, t.i. pull in push metodi. Podrobnejša razlaga načina delovanja ene in druge metode sledi v nadaljevanju.
2. Analiza dnevnikov
   Analiza je osrednji del vsakega sistema SIEM. Pri analizi se uporabljajo razni matematični in drugi logični prijemi. Analitični del v splošnem pozna naslednje prvine: razčlenjevanje, normalizacijo, združevanje, filtriranje ter izdelavo pravil in korelacij.
3. Hramba dnevnikov
   Za dnevnik je to zadnja faza njegovega življenjskega cikla. Večina ponudnikov SIEM omogoča dvonivojsko shranjevanje dogodkov. Prvi nivo hrambe je na sami SIEM namenski napravi, drugi pa predstavlja zunanji pomnilniški sistemi.

4.2 SIEM arhitektura

V nadaljevanju si bomo podrobneje pogledali posamezne dele SIEM arhitekture in njihove funkcije. Omenjene glavne tri naloge bomo še dodatno razčlenili (slika 10) ter jih podkrepili s primeri.



Slika 10: SIEM arhitektura

Viri

Začetni korak verige predstavlja nastavitev naprave oz. vira, ki generira dnevnike. Brez naprav oz. njihovega izvora dnevnikov tudi potrebe po sistemu SIEM ne bi bilo. Kot vir lahko razumemo vsako napravo ali sistem, ki generira neke dogodke. V to skupino sodijo operacijski sistemi, aplikacije, strežniški sistemi, omrežne in druge naprave. Če želimo, lahko v SIEM zajamemo tudi dogodke iz vseh delovnih postaj in prenosnikov. Priporočljivo je vključiti tudi dnevnike centralnega protivirusnega sistema in drugih pomembnih infrastrukturnih aplikacij (poštni strežnik, podatkovni strežnik, spletni strežnik, DNS, DHCP, idr.). Zelo pomemben vir informacij predstavljata sistem za zaznavanje vdorov (angl. intrusion detection system, krat. IDS) in sistem za preprečevanje vdorov (angl. intrusion prevention system, krat. IPS) [13]. Slednja nam še dodatno izboljšata pregled nad celotnim dogajanjem v informacijskem sistemu.

Zajem dnevnikov

Naslednji korak predstavlja zajem dnevnikov. V splošnem obstajata dva načina zajema dnevnikov: pull in push metoda.

Pri pull metodi je iniciator SIEM. Omenjeno predstavlja določeno prednost, saj je SIEM tisti, ki opravlja glavno vlogo in ima nad napravo tudi določeno kontrolo. Slaba stran te metode pa je, da se v večini primerov ne zgodi v realnem času. To pomeni, da SIEM dobi dnevnike z določenim zamikom.

Pri push metodi je naprava tista, ki začne s pošiljanjem dnevnikov. Ta način je značilen za omrežne naprave, ki svoje dnevnike hranijo v syslog formatu. Vse kar je potrebno storiti, je, da napravo usmerimo na syslog strežnik – v našem primeru je to kar sistem SIEM. Za naprave, ki ne poznajo syslog formata in svoj dnevnik shranjujejo v npr. navadno tekstovno datoteko, je potrebno uporabiti agenta. Agent je vrsta programske opreme, ki jo najprej namestimo na napravo in nato ustrezno nastavimo. Njegova naloga je, da dnevniške zapise pretvori v obliko oz. format, ki jo SIEM razume in jih posreduje v SIEM. Podrobnejša razlaga formatov sledi v poglavju 4.3.

Razčlenjevanje in normalizacija
Po uspešnem zbiranju dnevnikov iz različnih virov v centralno točko nastopi drugi problem: neenotnost dnevniških formatov. Vsak sistem SIEM ima svoj jezik oz. format s katerim izvaja vse nadaljnje operacije. Zato je potrebno vse dnevniške zapise postaviti na skupni imenovalec. Temu procesu pravimo normalizacija. Pred postopkom je potrebno najprej razčleniti posamezen dnevniški zapis. Če poenostavimo: dnevniški zapis najprej razčlenimo na polja in ga nato s postopkom normalizacije sestavimo v želeno obliko. Končni rezultat normalizacije je poenotenje vseh dnevnikov v en skupen format. Pri procesu normalizacije je mogoče normalizirati poljubno podatkovno polje v dnevniku.

Normalizacija se najbolj pogosto uporablja pri določanju enotne oblike datuma in časa.
Primer normalizacije datuma:

$$\left.\begin{array}{c} MM.DD.YY\ (09.20.11) \\ YY/MM/DD\ (11/09/20) \\ DD/MM/YYYY\ (20/09/2011) \end{array}\right\} DD.MM.YYYY\ (20.09.2011)$$

Pri poenotenju časa naletimo tudi na podoben problem. Upoštevati moramo ali je zapis v 12 ali 24-urnem formatu. Dodatna pazljivost je potrebna v primeru zajemanja dnevniških datotek iz različnih časovnih pasov.

Združevanje
Postopek združevanja se običajno izvede takoj za postopkom normalizacije. Gre za postopek združevanja enakih dogodkov. V primeru prihajanja večkratnih ponovitev istih dogodkov jih sistem SIEM sešteva in obravnava kot en sam dogodek. S tem se izognemo podvajanju zapisov v bazi in posledično skrbimo za optimizirano hrambo dogodkov.

Pravila in korelacije
Izdelava pravil in korelacij nastopi po normalizaciji. Dejstvo je, da si sistema SIEM ni mogoče predstavljati brez možnosti uporabe pravil in korelacij. S pravili si olajšamo delo pri pregledovanju ogromne količine dogodkov. Pogostokrat pa tudi za nadaljnje alarmiranje in obveščanje.

Pravilo sestavimo tako, da izberemo želena polja določenega dogodka ter z ustrezno logiko skušamo priti do uporabnih informacij, npr. da nekdo izvaja napad z grobo silo (angl. brute force attack). Nekaj osnovnih pravil premore vsak sistem SIEM, za vse ostale pa je potrebno izdelati lastna pravila. Običajno se pri pisanju pravil uporablja Boolova algebra.
Pravila so lahko povsem enostavna, lahko pa sestavimo tudi zelo zapleteno pravilo. Sledijo primeri z različno stopnjo težavnosti:

Primer 1: Prikaži vse dogodke domenskega strežnika

$$[(ponorni\ IP)\ OR\ (izvorni\ IP)]\ ==\ 10.10.10.25$$

Gre za dokaj enostavno pravilo, ki bi ga lahko realizirali tudi s filtriranjem dogodkov znotraj grafičnega uporabniškega vmesnika (angl. graphical user interface, GUI). Privzamemo, da je IP domenskega strežnika 10.10.10.25.

Primer 2: Prikaži vse domenske prijave v zadnjih 24 urah
V tem primeru smo zasnovali pravilo nad tremi informacijami (IP domenskega strežnika, uspešnost prijave in časom).

$$[ponorni\ IP\ ==\ (10.10.10.25)]\ AND\ [(uspešna\ prijava)\ OR\ (neuspešna\ prijava)]$$
$$znotraj\ Date(Today)\ -\ 1$$

Primer 3: Prikaži morebitne napade z grobo silo
Ta primer je že nekoliko kompleksnejši, ampak še vedno razumljiv in zelo uporaben pri vsakodnevnem spremljanju dogajanja v IS.

Pravilo v intervalu dvajsetih sekund išče tri (ali več) neuspele prijave ter takoj zatem še uspelo prijavo. V primeru, ko naleti na tako sosledje dogodkov, sproži alarm za morebiten napade z grobo silo. Več o alarmih in incidentih je govora v nadaljevanju.

$$IF\ [(neuspešna\ prijava\ \geq 3)AND\ Then\ (uspešna\ prijava)]\ iz\ istega\ izvornega\ IP$$
$$v\ intervalu\ 20\ sekund\ =>\ morebiten\ napad\ z\ grobo\ silo$$

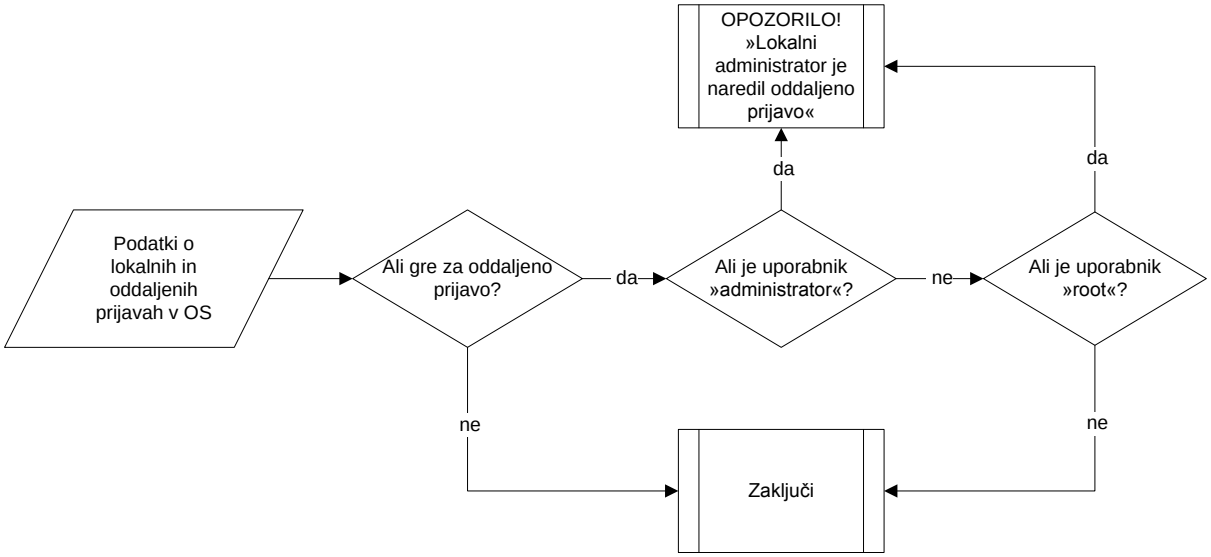
V tabeli 1 je prikazan dvajset sekundni zajem dogodkov. S sivo barvo so obarvani dogodki, ki ustrezajo zgornjemu pogoju.

Čas dogodka	ID dogodka	Izvorni IP	Ponorni IP	Opis dogodka
10:10:01 CEST	1035	192.168.1.200	10.10.10.25	neuspešna prijava
10:10:02 CEST	1036	192.168.1.90	10.10.10.21	uspešna prijava
10:10:04 CEST	1037	192.168.1.200	10.10.10.25	neuspešna prijava
10:10:06 CEST	1038	192.168.1.91	10.10.10.35	neuspešna prijava
10:10:07 CEST	1039	192.168.1.10	10.10.10.2	uspešna prijava
10:10:08 CEST	1040	192.168.1.10	10.10.10.3	uspešna prijava
10:10:10 CEST	1041	192.168.1.200	10.10.10.25	neuspešna prijava
10:10:11 CEST	1042	10.10.10.54	192.168.1.201	neuspešna prijava
10:10:14 CEST	1043	10.10.10.34	192.168.1.10	neuspešna prijava
10:10:17 CEST	1045	192.168.1.200	10.10.10.25	uspešna prijava
10:10:21 CEST	1046	192.168.1.191	10.10.10.21	uspešna prijava

Tabela 1: Primer zajema dogodkov v dvajset sekundnem intervalu

Primer 4: Prikaži oddaljene prijave lokalnih administratorjev na vseh tipih OS
Na primeru bomo pokazali kako lahko s pomočjo pravila izdelamo obveščanje, ki se sproži ob oddaljeni prijavi lokalnega administratorja na katerikoli sistem. Da bo pravilo neodvisno od tipa OS, moramo pri tem upoštevati tipična poimenovanja lokalnih administratorjev, ki so značilna za določen OS. V Windows svetu je to "administrator", v Linux svetu je "root" itd.

Torej bomo pravilo zasnovali tako, da bo neodvisno od tipa OS in naprave (strežnik, delovna postaja idr.). Pravilo je prikazano v obliki diagrama poteka (slika 11).



Slika 11: Diagram poteka – oddaljene prijave lokalnih administratorjev

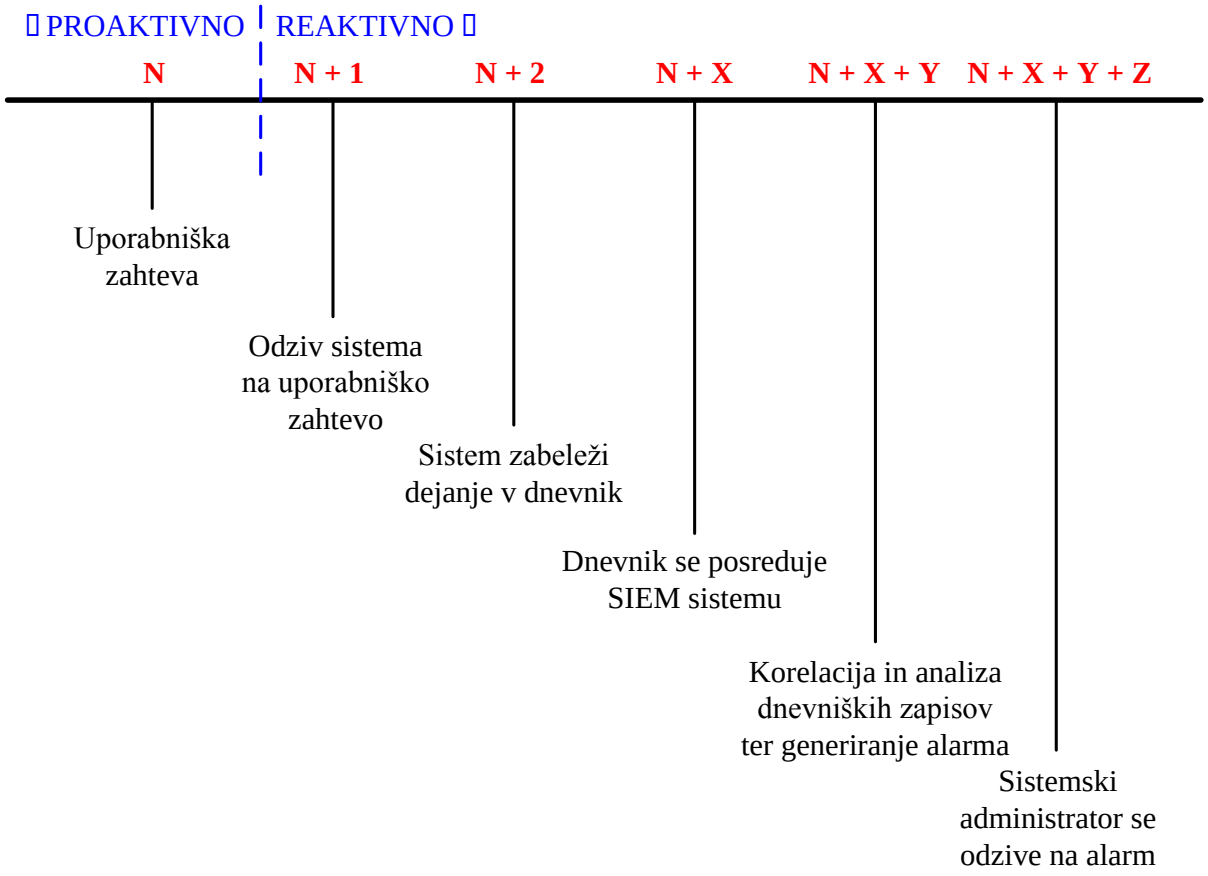
Na podlagi dogodkov, ki smo jih zbrali s primeroma 3 in 4, bomo prikazali še primer korelacije. S korelacijo dveh dogodkov o morebitnem napadu z grobo silo (primer 3) in opozorilom, da se je lokalni administrator prijavil preko oddaljene seje (primer 4), sprožimo alarmiranje. S takim pristopom pridobimo še dodatne informacije o napadu, saj obveščeni ve, da gre za poskus napada z lokalnim administratorjem preko oddaljene seje.

Alarmi, incidenti, poročila in spremljanje

Dodana vrednost vsakega sistema SIEM je alarmiranje v primeru zaznanih napadov in kršitev. Obstajajo štirje načini obveščanja:

a) Proženje alarmov
   Sistem se v primeru zaznanega napada takoj odzove z alarmom. Alarm je lahko v obliki elektronske pošte, SMS-a, opozorila v nadzorni plošči ipd.
b) Posredovanje incidentov
   SIEM ima možnost svoje alarme posredovati v storitveni center oz. aplikacijo za upravljanje incidentov.
c) Izdelava poročil
   Poročila se izdelujejo po določenem časovnem planu ali na zahtevo. Vsak sistem SIEM vsebuje že predpripravljena poročila, kar nam še dodatno olajša delo. Ena izmed rednih nalog sistemskih administratorjev je ravno pregledovanje teh poročil in ugotavljanje anomalij v IS.
d) Aktivno spremljanje dogajanja
   Spremljanje stanja IS v realnem času je ena izmed pomembnejših lastnosti sistema SIEM. Če te funkcionalnosti ne izkoristimo, pomeni, da je sistem namenjen le hrambi dnevnikov. Spremljanje dogajanja v realnem času nam omogoča nadzorna plošča z grafičnim vmesnikom. Preko nadzorne plošče imajo sistemski administratorji vpogled v morebitne alarme in incidente.

Primer na sliki 12 prikazuje časovno sosledje dogodkov v primeru alarma.



Slika 12: Časovni prikaz dogodkov v primeru alarma

N – trenutek, ko se zgodi uporabniška zahteva
X – čas, ki ga porabi SIEM za zajem dogodkov
Y – čas, ki ga porabi SIEM za korelacijo dogodkov
Z – čas, ki ga potrebuje administrator, da se odzove na alarm

Pomembno je, da je vsota časov čim manjša. Za zagotavljanje čim krajšega odzivnega časa je potrebno redno pregledovati vse tri čase (X, Y in Z).

Hramba dnevnikov
Življenjski cikel dnevnika se zaključi s postopkom shranjevanja. Dnevniki se shranjujejo v normalizirani obliki. Za potrebe dokazovanja skladnosti s standardi pa je potrebno dogodke hraniti tudi v njihovi originalni obliki.

Sistemi SIEM že v osnovi zagotavljajo določeno kvoto prostora, ki je namenjen hrambi dnevnikov. To je t.i. prvi nivo hrambe dnevnikov, ki je običajno v namenski SIEM napravi. Kvota je omejena glede na število diskov, ki jih je mogoče vgraditi v tako napravo (običajno je efektivnega prostora manj kot 1 TB). To pa nikakor ne zadošča za sedemletno hranjenje dnevnikov. Standardi in regulative zahtevajo večletno hranjenje dnevnikov (tabela 2). Zato večina SIEM rešitev predvideva vzpostavitev zunanjega nivoja hrambe (NAS, SAN idr.). Pri vzpostavitvi drugega nivoja hrambe je pomembno, da končna rešitev zagotavlja osnova načela informacijske varnosti (zaupnost, neokrnjenost in razpoložljivost).

Pri arhiviranju dnevnikov je pomembna tudi kompresija podatkov. Ponudnik RSA navaja, da njihov sistem enVision zmore tudi do 8-kratno kompresijo podatkov.

Standard	Čas hrambe (v letih)
PCI DSS	1
FISMA	3
NERC	3
GLBA	6
HIPAA	6
Basel II	7
SOX	7

Tabela 2: Predpisan čas hranjenja dnevnikov za določen standard

4.3 Format, transport in vsebina dnevnika

V tem poglavju si bomo ogledali katere formate, načine transporta in vsebine, ki jih srečujemo na področju upravljanja dnevnikov, na koncu pa dodali še nove smernice standardizacije.

V dobrih tridesetih letih se je pojavilo ogromno rešitev kako postaviti standarde na tem področju. Če je bilo še pred desetimi leti dovolj, da je bil dnevnik iz naprave A dostavljen sistemu B, potem v današnjem času temu ni tako. Vedno večji poudarek na varnosti je korenito spremenil tudi to področje. Zahteve po vgradnji varnostnih mehanizmov v proces prenosa podatkov in poenotenju formata so bile vse večje. To je še dodatno vzpodbudilo strokovnjake, da dokončno postavijo področne standarde.

4.3.1 Format

Format si lahko predstavljamo kot nekakšen jezik. Ta ima svojo sintakso, kar vključuje pravila in strukturo stavkov oz. v našem primeru dnevniških zapisov. V SIEM prihajajo dnevniki v različnih formatih. Proizvajalci namreč uporabljajo različne formate. Dogodki operacijskega sistema se zopet zapisujejo v drug format (Windows uporablja svoj format, UNIX sistemi uporabljajo syslog itd.). Ta široka paleta formatov predstavlja dodatno delo za SIEM. Če želi SIEM "razumeti" vse te različne zapise dogodkov, jih mora najprej razčleniti in normalizirati. Tu se izgublja dragoceni čas, ki bi ga lahko sistem izkoristil za hitrejšo analizo in alarmiranje.

Prednosti uporabe standardiziranega formata:
- s standardizacijo formata bi prihranili procesorski čas, ki ga SIEM porabi za razčlenjevanje in normalizacijo dnevnikov,
- krajši čas učenja sintakse,
- lažje razumevanje dnevniških zapisov in posledično lažja uporaba,
- lažje delo za zunanje skrbnike, programerje in revizorje,
- lažja komunikacija med dvema sistemoma SIEM.

V preteklosti je bilo kar nekaj neuspelih poskusov standardizacije. Omeniti velja:

a) Intrusion Detection Message Exchange Format (IDMEF)
Leta 2002 je organizacija Internet Engineering Task Force (IETF) predstavila študijo o novem formatu IDMEF [24]. Zasnovan je bil za IDS naprave. Format uporablja jezik XML. Za prenos podatkov pa skrbi protokol IDXP, ki ga je ravno tako predlagal IETF. Format ni bil dobro sprejet, glede na to, da danes le redko katera IDS naprava podpira ta format. Poskus standardizacije ni bil uspešen, saj so mu pripisali, da je format preveč osredotočen na IDS dogodke in ni splošno naravnan.

b) Security Device Event Exchange (SDEE)
Organizacija ICSA Labs je leta 2003 predlagala nov format SDEE, namenjen varnostnim napravam. Za transport uporablja protokol SOAP. Format, ki je bil zasnovan na osnovi XML je bil v prvi vrsti namenjen IDS napravam, s poudarkom na razširljivosti. Cisco je to izkoristil in izdelal dodatek, ki ga je uporabil za svojo linijo IPS sistemov. Tako je nastal nov protokol Cisco Intrusion Detection Event Exchange (CIDEE). Razen omenjene svetle izjeme SDEE ni zabeležil večjih uspehov.

c) Common Event Format (CEF)
Septembra 2006 je podjetje ArcSight predstavilo svoj format, imenovan Common Event Format. CEF je enostaven za uporabo, saj uporablja navadno besedilo kodirano po načinu UTF-8 in ni odvisen od načina transporta. Polja so med seboj ločena z znakom "|".

Splošen primer uporabe CEF formata:

CEF: Version|Device Vendor|Device Product|Device Version|
Signature ID|Name|Severity|
Extension

Omeniti velja, da je polje "Extension" sestavljeno iz obsežne množice parov, ki jih tvorita ključ, enačaj ("=") in njegova vrednost.

Primer zapisa, ko je naprava "threatmanager" uspešno zaustavila črva, ki je vršil promet po vratih 1232 iz 10.0.0.1 proti 198.168.2.2, bi v CEF formatu izgledal:

CEF: 0|security|threatmanager|1.0|
100|worm successfully stopped|10|
src = 10.0.0.1 dst = 198.168.2.2 spt = 1232

ArcSight ni zaščitil formata, temveč ga je ponudili ostalim proizvajalcem v želji, da se ta razširi. Njihova prizadevanja, da bi CEF postal uradno priznani standard, niso uspela. Vseeno jim je uspelo vzpodbuditi nekatere organizacije, da so pričele uporabljati CEF (IBM, Imperva, Cyber-Ark, FairWarning, ForeScout idr.).

d) Common Base Event
Tudi IBM je razvil svoj format (CBE). Zasnovan je na osnovi XML in se uporablja v IBM Tivoli rešitvah, ter nekaterih Cisco produktih. Ostali proizvajalci formata niso podprli.

e) WebTrends Enhanced Log file Format (WELF)

Format je razvilo podjetje WebTrends. Razširjen je predvsem v sektorju proizvajalcev požarnih pregrad. Uporaben je še za posredovalne strežnike (angl. proxy) in IDS naprave.

4.3.2 Transport

Brez transporta oz. prenosa sporočil bi dnevniki ostali na napravi oz. sistemu, ki ga je generiral. Za učinkovit transport dogodkov oz. podatkov mora standard zagotavljati osnovna načela informacijske varnosti kot so zaupnost, neokrnjenost in razpoložljivost. V nadaljevanju si bomo pogledali tri standarde, ki se uporabljajo še danes.

a) Simple Network Management Protocol (SNMP)
   Preprosti protokol za upravljanje omrežja SNMP je leta 1988 definirala organizacija IETF. Od takrat predstavlja industrijski standard za nadzor in upravljanje omrežnih naprav. Nadgradnja protokola, znana kot SNMPv2c, ki je izšla leta 1993, je nudila podporo za centralizirane in porazdeljene upravljalne strategije. Ob tem pa je vsebovala še dodatne posodobitve. Leta 2004 je bil izdan SNMPv3. V tretji verziji SNMP protokola so še dodatno izboljšali varnostne mehanizme, saj zagotavlja vsa tri osnovna načela informacijske varnosti.

   SNMP predstavlja nabor omrežnih protokolov in funkcij za nadzor omrežja, ki komunicirajo z uporabo IP sklada. SNMP omogoča skrbniku omrežja, da izolira in odpravi napake v omrežju, ki ga sestavljajo naprave različnih proizvajalcev, konfigurira naprave v omrežju, hkrati pa omogoča pregled in nadzor nad učinkovitostjo omrežja. Omogoča nadzor nad veliko količino sistemskih funkcij v posameznih napravah. Obenem je tudi neodvisen od operacijskega sistema. Deluje na aplikacijskem nivoju modela OSI. Za komunikacijo uporablja protokol UDP (vrata 161 in 162). Slednji je izpostavljen raznim napadom (npr.: potvarjanje IP naslova, angl. IP spoofing). Kot že rečeno, so te varnostne ranljivosti odpravili v tretji verziji SNMP.

b) Syslog
   Syslog ima že več kot tridesetletno zgodovino. Vse od leta 1980 pa do 2001 je bil syslog de facto standard. Leta 2001 pa ga je organizacija IETF standardizirala (RFC 3164). Danes je v veljavi RFC 5424.
   Syslog je priznan s strani organizacije NIST kot standard za zapisovanje dnevniških zapisov.

   Vsak syslog dnevniški zapis je sestavljen iz treh delov:
   - Glava
     - prioriteta
     - syslog verzija
     - časovni žig
     - IP naslov ali FQDN naziv izvora
     - ime naprava ali aplikacije, ki je generirala dogodek
     - ime procesa ali ID procesa
     - tip dogodka

     V glavi so polja med seboj ločena s presledki.
   - Strukturirani podatki

Ti so navedeni takoj za glavo in sicer z znakom "[", končajo pa z znakom "]". Znotraj teh znakov so definirani pari, ki jih tvorijo ključ, enačaj ("=") in njegova vrednost.

- Opis
  Gre za podrobnejši opis dogodka. Pri tem moramo upoštevati, da je maksimalna dolžina enega zapisa 1024B.

Za komunikacijo uporablja protokol UDP (vrata 514). Klasični primer komunikacije je med napravo in syslog strežnikom ali pa napravo in sistemom SIEM (ali pa katerim drugim nadzornim orodjem). Transport syslog sporočil (RFC 3164) ni imel vgrajenih nobenih varnostnih mehanizmov, vse do RFC 3195, ki zagotavlja načela zaupnosti, neokrnjenosti in razpoložljivosti.

Zaupnost lahko zagotovimo z uporabo protokola TLS. Pri uporabi TLS naletimo na omejitev, saj lahko razen glave zaščiti celoten zapis. Če želimo zaščititi tudi glavo, potem je potrebno uporabiti program, ki zna vzpostaviti SSH tunel med napravo in strežnikom syslog (npr.: PuTTY, Stunnel, sslio, sslwrap idr.).

Neokrnjenost sporočila zagotovimo z uporabo zgoščevalne funkcije MD5 oz. SHA. To še posebej velja, za organizacije, ki morajo biti skladne po standardu FIPS. Za zagotavljanje razpoložljivosti oz. dostavljivosti paketa lahko poleg UDP uporabimo še protokol TCP.

c) Intrusion Detection Exchange Protocol (IDXP)
   Protokol IDXP je namenjen izmenjavi podatkov med napravami IDS. Predlagala ga je organizacija IETF (RFC 4767). IDXP podpira vzajemno preverjanje pristnosti, neokrnjenosti in zaupnosti. Protokol je bil namenjen transportu IDMEF sporočilom.

4.3.3 Vsebina

To področje se ukvarja z vsebino dnevnikov in z razlago vsebine – kaj določeno polje pomeni. Standardizacija na tem področju je otežena zaradi množice različnih naprav in sistemov, ki generirajo "nestandardne" dnevnike. V nadaljevanju je omenjen en osamljen poskus standardizacije na tem področju.

a) Common Intrusion Event List (CIEL)
   Eden redkih poskusov po standardizaciji vsebine dnevnika je bil leta 2001 s strani organizacije MITRE. Gre za projekt Common Intrusion Event List. CIEL je bil namenjen upravljanju dogodkov iz sistemov za zaznavanje vdorov. Zaradi preozke specializiranosti in kompleksnosti je bil prekinjen nadaljnji razvoj standarda.

4.3.4 Nove smernice

V nadaljevanju si bomo pogledali format, ki mu je uspelo postaviti standarde na tem področju. Gre za projekt Common Event Expression (CEE).

CEE je dolgo pričakovani standard na tem področju. Začetki projekta segajo v leto 2007. Standard, ki je pod okriljem organizacije MITRE zorel vsa ta leta, je pridobival vse več

privržencev in strokovnjakov, ki so bili pripravljeni pripeljati zgodbo do konca. To jim je leta 2011 tudi uspelo. Uspeli so pripraviti standard, ki ni odvisen niti od izvorne naprave (tj. tista, ki generira nek dogodek), niti od ponorne naprave (SIEM, syslog strežnik idr.). Skratka, standard je zasnovan za široko uporabo.

Arhitektura standarda je sestavljena iz štirih komponent.

- Slovar in taksonomija
  Na začetku je potrebno zgraditi t.i. slovar in ustrezne relacije med posameznimi kategorijami. Trenutno je slovar sestavljen iz 20-ih podatkovnih množic in 128 polj. Taksonomija pa vsebuje 85 oznak, ki pripadajo šestim kategorijam. Taksonomija predstavlja urejenost in hierarhijo jezika. S slovarjem pa obogatimo sam jezik. Ko povežemo vsa polja nekega dogodku s polji v slovarju in določimo taksonomijo, se lahko lotimo izbire najprimernejše sintakse.

- Sintaksa
  Na podlagi definiranega slovarja, bo možno izbirati med več sintaksami (binarna oblika, navadno besedilo, XML, JavaScript Object Notation in syslog). CEE standard znova pušča odprte roke pri izbiri sintakse. Večina jih je mnenja, da je XML oblika najprimernejša za opis dogodkov. Po drugi strani pa bolj bremeni promet po omrežju kot binarna oblika zapisa ali pa navadno besedilo.

- Transport oz. prenos
  CEE ne predpisuje uporabe točno določenega protokola, ker bi se s tem omejil. Raje je prepustil odločitev proizvajalcem, da sami izberemo vrsto protokola. Ima pa podporo za vse aktualne načine transporta (syslog, SNMP, IDXP, HTTPS, SQLNet idr.). Da bi bila zadeva še bolj splošna, CEE podpira tri tipe prenosa:
  a) Hiter. Tega načina se poslužujemo, če imamo za prenos podatkov po mreži premalo pasovne širine. Podatki so v binarni obliki, kar je odlično za hitrost prenosa, za administratorja pa neuporabno oz. neberljivo.
  b) Enostaven. Podatki so shranjeni v obliki navadnega besedila (glej CEF). Gre za najbolj pogost in podprt način prenosa, ki je že dobro sprejet med SIEM proizvajalci.
  c) Izrazen. Podatki so v XML obliki (glej SDEE, CBE). Avtorji menijo, da ni potrebe po XML obliki, češ da je veliko bolj praktična in razširjena oblika, ki uporablja navadno besedilo.

- Priporočila
  Namenjena so vsem, ki se bodo ukvarjali z implementacijo tega standarda.

Tu velja omeniti še dva protokola, ki sta pred kratkim naredila velik korak naprej na področju poenotenja formatov.

a) Security Content Automation Protocol (SCAP)
   Organizacija NIST je februarja 2011 izdala verzijo 1.1 standarda SCAP. SCAP predstavlja skupek odprtokodnih standardov, ki omogočajo avtomatizirano zaznavanje ranljivosti, napačnih konfiguracij, merjenje in ugotavljanje skladnosti (npr.: FISMA). SCAP je še veliko več kot to, njegove metode se še uporablja pri:
   - odkrivanju varnostnih lukenj v programski opremi,
   - odkrivanju napačnih oz. spornih sistemskih varnostnih nastavitev,
   - odkrivanju imena produktov,
   - spremljanju internih politik in skladnosti s standardi,

- meritvah,
- ocenjevanju vpliva najdenih varnostnih groženj.

Poleg kataloga ranljivosti, napačnih nastavitev in imena produktov, SCAP prinaša novi funkcionalnosti, meritve in sistem točkovanja. Na podlagi meritev ranljivosti in sistema točkovanja zna izračunati stopnjo ogroženosti za določen sistem. SCAP standardi imajo za svojo referenčno točko ameriško nacionalno bazo ranljivosti (angl. National Vulnerability Database). Baza vsebuje podatke o varnostnih ranljivostih, napačnih nastavitvah, imenih izdelkov in razne metrike. Dnevno se doda 20 novih ranljivosti, kar predstavlja več kot 6000 na leni ravni.

SCAP združuje 7 odprtih standardov [35]:

- Common Vulnerabilities and Exposures (CVE): namenjen odkrivanju varnostnih lukenj in groženj v programski opremi,
- Common Configuration Enumeration (CCE): namenjen odkrivanju napak v konfiguraciji sistemov,
- Common Platform Enumeration (CPE): namenjen poimenovanju produktov,
- Common Vulnerability Scoring System (CVSS): sistem za točkovanje varnostnih ranljivostih,
- Extensible Configuration Checklist Description Format (XCCDF): namenjen poročanju o rezultatih vrednotenja sistemov,
- Open Vulnerability and Assessment Language (OVAL): namenjen poročanju o odkritih varnostih ranljivostih in konfiguracijskih napak.

Standard		Katalog	Ocenjevanje	Merjenje	Poročanje	Vsebina
cve.mitre.org	**CVE**	●				●
cce.mitre.org	**CCE**	●				●
cpe.mitre.org	**CPE**	●				●
cvss	**CVSS**			●		●
XCCDF security benchmark automation	**XCCDF**		●		●	●
oval.mitre.org	**OVAL**		●		●	●

Tabela 3: Pregled standardov SCAP in njihov namen

b) Event Management Automation Protocol (EMAP)
Meseca junija 2011 je organizacija NIST uradno izdala zbirko zbranih specifikacij EMAP, ki urejajo standardizacijo sporočanja na področju upravljanja dogodkov. Če je SCAP zbirka standardov na področju ranljivosti in konfiguracij, potem je EMAP

njegov dvojček, ki pokriva področje upravljanja dogodkov. EMAP za transport uporablja standard CEE, ki smo ga opisali na začetku poglavja. Trenutni razvoj standarda gre v smeri povezovanja EMAP in SCAP.

EMAP je sestavljen iz naslednjih komponent:

- generator dogodkov,
- delo z nestandardnimi formati,
- orodje za razčlenjevanje,
- definicija razčlenjevalnih pravil,
- definicija dnevniških zapisov,
- hramba dogodkov,
- orodje za korelacijo,
- definicija korelacijskih pravil,
- orodje za filtriranje,
- definicija pravil za filtriranje,
- orodje za združevanje,
- definicija pravil za združevanje,
- politika upravljanja dogodkov,
- kategorizacija dogodkov.

EMAP komponente so hkrati glavne naloge SIEM (poglavje 4.2). V prihodnje je pričakovati vedno večjo podporo standardu s strani razvijalcev sistema SIEM.

5. Vzpostavitev sistema SIEM

Vzpostavitev sistema SIEM je kompleksen projekt, ki zahteva obsežne priprave in načrtovanja. Zaradi dodatne kompleksnosti, ki jo uvajamo v IS, je potrebno, da k projektu pristopijo vsaj naslednji člani: projektni vodja, direktor informatike, varnosti inženir, skrbnik omrežja, sistemski inženir, skrbnik podatkovnih baz, tehnolog, varnosti pooblaščenec, revizor, operater in v določenih primerih tudi zunanji (pogodbeni) izvajalec. Podrobnejša dodelitev vlog sledi v nadaljevanju (poglavje 5.2.1.1).

Kot pri vsakem projektu je tudi tu pomembno, da znamo oceniti stroške. Vodstvo pri tem predvsem zanimajo kazalci donosnosti naložbe (angl. return on investment, krat. ROI). Projekt bo odobren le v primeru, če bodo celotni stroški manjši od donosnosti naložbe.

5.1 Razlogi za SIEM

Podjetja, ki so se odločila za vpeljavo SIEM rešitve, so spoznala, da so v današnjem času protivirusna zaščita, požarna pregrada (angl. firewall), IDS sistemi, enostavno premalo za zagotavljanja želene stopnje varnosti. V nadaljevanju bomo navedli oba glavna razloga, zakaj se podjetja odločijo za vpeljavo SIEM rešitve.

a) Zagotavljanje skladnosti (angl. compliance)
Za večino podjetij je to glavni motivator, da se odločijo za vpeljavo sistema SIEM. Strošek "ročnega" preverjanja in izdelave poročil je nekajkrat višji od same SIEM implementacije. Strošek je še višji v primeru, da podjetje krši določene predpise oz. regulative.

SIEM proizvajalci ponujajo organizacijam že predpripravljena poročila za določene standarde. Nabor podprtih standardov je velik in se vsako leto širi, npr.: ISO/IEC 27001, Basel II, PCI DSS, SOX, GLBA, HIPAA idr. Od proizvajalca je odvisno ali bodo t.i. skladnosti paketi (angl. compliance modul) že vključeni v osnovno postavitev, oz. je potrebno zanje dodatno plačati.

b) Obvladovanje groženj (angl. threat management)
Organizacije se zavedajo nevarnosti, ki jim grozijo s tem, ko so izpostavljene najrazličnejšim napadom. Danes poznamo celo vrsto načinov kako se ubraniti pred morebitnimi napadi. Produkti kot so protivirusna zaščita, požarna pregrada, IDS in IPS sistemi so sestavni deli informacijske varnosti. Administrator ima pri pregledovanju dogodkov iz teh naprav oteženo delo, saj ima praviloma vsak produkt svojo nadzorno ploščo. Ideja sistema SIEM je, da v realnem času zajame in združi vse dogodke iz teh sistemov v enotno bazo. Moč takega sistema je ravno v širini informacij, ki jih zna zajeti in analizirati. Ta širina omogoča boljši pregled nad dogajanjem v IS.

Dejstvo je, da grožnje ne prihajajo samo iz zunanjega sveta, temveč tudi od znotraj. Gre za t.i. notranje grožnje (angl. internal threats). S pomočjo podpornih funkcij, ki smo jih našteli v prejšnjem poglavju, lahko spremljamo vsa dejanja, ki jih naredi uporabnik znotraj IS. Še posebej se velja osredotočiti na nadzor priviligiranih oz. administratorskih računov in njihovo vedenje.

V primeru zaznane grožnje (zunanje in notranje) ima sistem SIEM vpeljane postopke za upravljanje z incidenti.

Večkrat pa sta prisotna oba razloga, saj je v splošnem želja vsake organizacije, da je skladna s predpisi in uspešno obvladuje grožnje. Na to dejstvo opozarjajo tudi letne raziskave podjetja SANS [34].

V nadaljevanju sledi opis postopkov, ki so potrebni pred vzpostavitvijo.

5.2 Postopki pred vzpostavitvijo

V tem poglavju bomo skušali podati osnovne smernice, ki jih je priporočljivo upoštevati pred vzpostavitvijo sistema SIEM.

Raziskovalno podjetje SANS priporoča, da si pred vzpostavitvijo postavimo naslednjih 5 vprašanj (five W's) [26]:
Why (zakaj) – Zakaj želimo vzpostaviti SIEM? Kaj je glavni motivator?
Who (kdo) – Kdo bo sodeloval pri projektu?
What (kaj) – Kaj želimo doseči? Kaj pridobimo z vzpostavitvijo sistema SIEM?
Where (kam) – Kakšen bo obseg rešitve (regionalna, distribuirana, visoko razpoložljivostna rešitev)?
When (kdaj) – Kdaj bo projekt zaključen in v kolikšni meri?

5.2.1 Organizacija

Najprej se moramo na nivoju organizacije vprašati zakaj želimo vzpostaviti sistem SIEM. Organizacije si v splošnem od SIEM obetajo izboljšave na naslednjih področjih: preverjanje skladnosti, odkrivanje zunanjih in notranjih napadov, upravljanje dnevnikov, upravljanje dogodkov, upravljanje incidentov, forenziki, upravljanje identitet, idr.

Za izbran produkt je pomembno, da ustreza velikosti podjetja, načinu in obsegu poslovanja, sredstvih, organizacijski kulturi ter znanju. Končna postavitev SIEM mora temeljiti na ciljih organizacije. Vsekakor je na prvem mestu vzpostavitev želenega nivoja informacijske varnosti v organizaciji, ki temelji na SUVI. Sem spada poznavanje internih politik in aktov organizacije, ter jasna določitev vlog in pristojnosti posameznikov. Poznavanje internih politik je ključna za pravilno izbiro produkta. Tu odigra pomembno vlogo (notranji) revizor.

V splošnem mora biti SIEM tako naravnan, da kar najbolje služi strategiji organizacije in pri tem ne ovira njenega poslovanja.

5.2.1.1 Vloge

Razdelitev vlog v veliki meri vpliva na velikost organizacije. Večja kot je organizacija, večje je število vlog in njihovih članov. Standarda NIST SP 800-92 in 800-100 predlagata naslednje vloge:

- Direktor informatike (angl. chief information officers, krat. CIO) je odgovoren za interno politiko beleženja dogodkov in za zagotavljanje skladnosti s predpisi in internimi akti. Odobri izvedbo izobraževanja za zaposlene in se dogovori za morebitno testno postavitev sistema.

- Skrbnik sistema SIEM je običajno sistemski skrbnik. Slednji ima veliko odgovornost, saj skrbi za vse faze delovanje (zajem, analizo in hrambo podatkov). Ravna se po predpisih varnostne politike beleženja. Znotraj sistema SIEM ima pregled in pravico dodeljevanja pooblastil posameznim članom, nad katerimi redno izvaja preglede in skrbi, da ne pride do zlorab.

- Upravljalec incidentov (angl. incident handler) je zadolžen za obravnavo incidentov. Ima dober pregled nad arhitekturo IS, pozna različne OS, omrežne protokole, forenzične veščine idr. Zaradi širokega spektra znanja je nepogrešljiv člen celotne verige. V primeru alarma aktivno sodeluje z ekipo za upravljanje incidentov.

- Sistemski administrator je odgovoren za konfiguracijo zajema dogodkov iz OS in aplikacij do katerih ima pooblastila. Vsakodnevno pregleduje dogodke za sisteme in poroča skrbniku v primeru anomalij.

- Skrbnik omrežja ima ekvivalentno vlogo kot sistemski administrator, le da je ta pooblaščen za omrežno opremo.

- Varnosti inženir je zadolžen za konfiguracijo varnostnih naprav (požarna pregrada, IDP/IPS idr.). Aktivno sodeluje z ostalimi člani pri konfiguraciji in optimizaciji nastavitev.

- Ekipa za upravljanje incidentov (angl. incident response team) skrbi za ustrezno rokovanje z incidenti. Ima nalogo stalnega spremljanja dogajanja in ustreznega reagiranja v primeru alarma. Ekipo lahko sestavljajo upravljavci incidentov, sistemski administratorji, skrbniki omrežja, člani centra za pomoč uporabnikom (angl. help desk), operaterji in drugi strokovnjaki. Med redne naloge spada izdelava poročil o incidentih za skrbnika sistema SIEM.

- Programer lahko s svojim znanjem ustrezno prilagodi aplikacijo, da ustreza varnostni politiki beleženja dogodkov.

- Revizor je tisti, ki pregleduje upoštevanje internih politik in skladnosti s predpisi. V času postopka je prisoten tudi skrbnik sistema SIEM.

5.2.2 Produkt

Pred izbiro produkta je smiselno postaviti testno postavitev (ti. pilot). Na ta način se še pred nakupom seznanimo s produktom. Pilot je predmet pogodbe z izvajalcem, ki ne sme biti zavezujoča. Podrobnejši pregled in primerjava produktov, ki smo jih izvedli v pilotski fazi, sledi v poglavju 6.4.

5.2.3 Proizvajalec

Pri izbiri proizvajalca je priporočljivo, da izberemo proizvajalca, ki je že prisoten ali vsaj delno prisoten v našem IS. V večini primerov to pomeni večjo kompatibilnost z obstoječo omrežno opremo in posledično lažjo integracijo sistema SIEM. V nadaljevanju sledi nekaj primerov takšnega sodelovanja.

a) HP strežniki in delovne postaje
   ArcSight je eno vodilnih ponudnikov SIEM rešitev. Septembra 2010 je podjetje HP kupilo ArcSight. Naložba je bila vredna 1,5 bilijona ameriških dolarjev. HP je za javnost izjavil, da bodo z nakupom vodilne SIEM tehnologije, še dodatno izboljšali obstoječi varnostni portfelj. HP-jeva odločitev se je izkazala za odlično, saj je podjetje ArcSight že šesto leto zapored zmagovalec v kategoriji SIEM. Raziskavo je vodilo raziskovalno podjetje Gartner.

b) EMC pomnilniški sistemi
   Podjetje EMC je že več kot desetletje v samem vrhu na področju visoko zmogljivih pomnilniških sistemov (angl. high-end storage systems). Septembra 2006 je podjetje kupilo kar dve podjetji: RSA za 2.1 bilijona ameriških dolarjev in njegovo hčerinsko družbo Network Intelligence za 175 milijonov ameriških dolarjev. Da je bila poteza EMC pravilna, namiguje dejstvo, da je bilo podjetje Network Intelligence še istega leta imenovano za vodilno podjetje na področju SIEM.

c) Cisco omrežna oprema
   Cisco je vodilno podjetje na področju omrežnih naprav. Leta 2005 na bilo podjetje na dobri poti, da s svojo SIEM rešitvijo Monitoring, Analysis, and Response System (MARS) še dodatno izkoristi svojo premoč na svetovnem trgu. Ampak štiri leta kasneje je prišlo do nepričakovanega obrata. Cisco se je leta 2009 odločil, da MARS ne bo več podpiral omrežnih naprav drugih proizvajalcev [25]. Od tu dalje je šlo vse samo še navzdol: padla je prodaja, ter MARS je izpadel iz Gartnerjevega magičnega kvadranta. Cisco je 3. junija 2011 dokončno naznanil konec prodaje sistema MARS.

Zadnji primer (propad sistema Cisco MARS) nakazuje, da obstajajo tudi manj posrečene izbire proizvajalca. Take vrste odločitev je težko vnaprej predvideti. Zato je toliko bolj pomembno, da pri izboru proizvajalca upoštevamo podatek do kdaj nudijo podporo za določen produkt.

Naslednji faktor, ki igra vlogo pri izboru proizvajalca, so njihove izkušnje in reference. Verjetnost, da bomo prej zaupali podjetju z več izkušnjami in referencami je bistveno višja kot pa sklenitev posla z začetnikom oz. "neznancem" na tem področju.

5.2.4 Omrežje

Poleg tega, da je produkt skladen z željami organizacije, je pomembno, da je rešitev primerna za interno omrežje organizacije. Pri vzpostavitev sistema SIEM je eden izmed ključnih dejavnikov uspeha dobro poznavanje omrežja. To še posebej velja pri velikih informacijskih okoljih. Poznavanje omrežja pripomore k skrajšanju časa implementacije.

Pred vzpostavitvijo sistema je pomembno, da skrbnik omrežja pripravi celoten seznam aktivne opreme. Šele za tem se skupaj z ostalimi člani projekta odločimo iz katerih naprav želimo zajemati dnevnike. To je še en dejavnik, ki vpliva na kompleksnost končne rešitve. Poleg tega pa večje število naprav predstavlja večje število dogodkov na sekundo (angl. events per second, krat. EPS), ki jih mora SIEM obdelati. V splošnem je parameter EPS določen s tipom licence, ki jo zakupimo za določen SIEM produkt.

Dodatna zahteva, ki jo mora izpolniti izbrani sistem je možnost nadgradnje sistema. Sem sodi dodajanje novih naprav in funkcionalnosti.

Projektna skupina se mora odločiti ali se bodo podatki filtrirali ali ne. Gre za pomembno odločitev, ki bo vplivala na količino podatkov. Velika količina podatkov predstavlja neposredno obremenitev omrežja in poslabšanje njenih performanc.

Skozi celoten proces vzpostavitve je potrebno aktivno sodelovanje skrbnikov omrežja. Velikokrat je predpogoj za zajem dnevnikov ustrezna konfiguracija požarne pregrade. Za uspešen zajem Windows dnevnikov s pull metodo in WMI (angl. Windows Management Instrumentation) ukazi je potrebno predhodno konfigurirati požarno pregrado, ter odpreti ustrezna vrata.

5.3 Zagotavljanja varnosti

S postavitvijo sistema SIEM se nam odpirajo nova varnostna vprašanja. Glede na občutljivo naravo podatkov, ki se hranijo oz. zbirajo v SIEM napravah, mora sistem zagotavljati ustrezno šifriranje podatkov. Obvezna je tudi avtentikacija uporabnika. Standard NIST SP 800-92 [21] predlaga vzpostavitev osnovnih načel informacijske varnosti: zaupnost, neokrnjenost in razpoložljivost - poznano kot CIA triada (angl. confidentiality, integrity and availability).

Zaupnost
Definicijo zaupnosti bi lahko strnili v "samo pooblaščene osebe lahko vidijo oz. imajo dostop do zaščitenih podatkov". Zaupnost pomeni omogočanje dostopa do podatkov, računalniških virov ter delov računalniškega sistema le pooblaščenim osebam. Omejevanje dostopa dosežemo s pooblaščenim dostopom in šifriranjem podatkov.

Neokrnjenost (neoporečnost, celovitost, integriteta)
V informacijski varnosti neokrnjenost podatkov pomeni, da podatki ne smejo biti ustvarjeni, spremenjeni ali uničeni brez predhodnega pooblastila.

Primer: Do izgube neokrnjenosti pride v primeru, ko sistem ni korektno ugasnjen, oz. ko spletni strežnik nenadoma izgubi električno energijo. Izguba neokrnjenosti pomeni tudi nenameren ali zlonameren izbris dnevnikov. Slednje je pogosto dejanje napadalcev, ki želijo za sabo počistiti sledi vdora.

Razpoložljivost (dostopnost)
Koncept razpoložljivosti predstavlja delujoči IS, ki obdeluje informacije. Za zagotavljanje razpoložljivosti je potrebno vzpostaviti določene varnostne kontrole [3], ki skrbijo, da so informacije razpoložljive in sistemi pravilno delujejo. Nasprotje razpoložljivosti je nedostopnost storitve oz. informacij.

Poseben varnosti izziv predstavljajo notranje zlorabe pooblastil. Te vrste zlorab je izredno težko preprečiti, saj imajo zaposleni s pooblastilom za uporabo SIEM vse pristojnosti za delo s sistemom. Edino kar lahko v tem primeru storimo je, da redno pregledujemo dnevniške zapise sistema SIEM. Še vedno se pa poraja večno vprašanje: "Kdo nadzoruje nadzornega?".

Poleg varovanja arhiviranih dnevnikov je potrebno zagotoviti tudi šifriranje dnevniških datotek med samim prenosom, kar pomeni od izvora (vir) do ponora (SIEM). Področje transporta in njegove varnostne mehanizme smo podrobneje obravnavali v poglavju 4.3.2.

5.4 Viri

Viri predstavljajo vhodni podatek za vsak sistem SIEM. V tem poglavju bomo skušali odgovoriti na vprašanje, katere vire je potrebno zajeti pri vzpostavitvi sistema SIEM. V grobem obstajajo trije viri: naprave, operacijski sistemi in aplikacije.

Naprave
Med naprave uvrščamo omrežno opremo, požarno pregrado, IDS/IPS sisteme, mobilne naprave, tiskalnike idr.

Požarni zid predstavlja osnovno informacijsko zaščito omrežja. Služi kot učinkovita zaščita notranjega omrežja (LAN) pred vdori iz zunanjega omrežja (WAN). Požarna pregrada je običajno postavljena na stičišče povezave med notranjim omrežjem in zunanjim svetom (internetom). Večji ponudniki požarnih pregrad: Cisco, Juniper Networks, Netgear, Nortel, Symantec, Fortinet, Check Point, McAfee, WatchGuard, SonicWALL idr.

IDS/IPS sistemi imajo nalogo, da nadzorujejo promet in dogodke v omrežju. Sistemi s pomočjo interne baze znanja, skenirajo promet v ključnih delih omrežja in iščejo morebitne napade. Zaznavanje napadov poteka na dva načina:

- prepoznavanje na osnovi podpisov, primerjanje določenih vzorcev dogajanja v omrežju z znanimi scenariji napadov (interna baza znanja),
- zaznava anomalij na podlagi ustvarjenih vzorcev običajnega vedenja omrežja, sistem prepozna in opozori na vsa odstopanja od običajnega vedenje.

Primer souporabe informacij iz IDS/IPS sistemov in požarne pregrade pri odkrivanju napadov: IDS in IPS sistema vsebujeta informacije o napadih, medtem ko informacije iz požarne pregrade lahko uporabimo pri ugotavljanju aktivnih povezav z zunanjim svetom (napadalčev računalnik).

Zanimivo je tudi spremljanje aktivnosti nad perifernimi napravami (tiskalniki, multifunkcijske naprave idr.). S spremljanjem lahko ugotovimo kdaj je neka naprava ugasnjena oz. celo v okvari. Poleg tega je mogoče iz informacij, ki jih vsebujejo dnevniki, pripraviti razna poročila (npr.: število natisnjenih strani na dan oz. kdo je natisnil največje število strani v določenem mesecu).

Operacijski sistemi
Sistemi SIEM podpirajo zajem dogodkov iz različnih OS. Tip strojne opreme na katerem teče OS ne igra posebne vloge – lahko je delovna postaja, prenosnik ali strežnik. Za SIEM je pomembna le različica OS. Tabela 4 prikazuje uporabo različnih OS skozi štiri letno obdobje [33]. Iz podatkov lahko ugotovimo, da imajo največji delež Windows OS (več kot 80%), sledijo mu Mac, Linux in mobilne naprave (iPad, Android, iPhone idr.).

	Win7	**Vista**	**Win2003**	**WinXP**	**Linux**	**Mac**	**Mobile**
junij 2008	/	10,0%	1,9%	74,6%	3,7%	4,8%	/
junij 2009	1,6%	18,3%	1,7%	66,9%	4,2%	5,9%	/

junij 2010	19,8%	11,7%	1,3%	54,6%	4,8%	6,8%	/
junij 2011	37,8%	6,7%	0,9%	39,7%	5,2%	8,1%	0,9%

Tabela 4: Statistični podatki o uporabi OS

Tržni delež OS Windows 7 se hitro povečuje in je tik pred tem, da prehiti najbolj popularen Microsoftov OS – Windows XP. Slednji bo 24. avgusta praznoval deseto obletnico obstoja.

Windows OS generirajo različne tipe dnevnikov. Vsak Windows OS generira vsaj naslednje tipe dogodkov:

- Aplikacijski dogodki
  OS obravnava dogodke glede na njihovo resnost. Obstajajo tri vrste aplikacijskih dogodkov: napaka, opozorilo in informacija. V primeru napake gre za resen problem, kot je npr. izguba podatkov. Opozorilo je dogodek, ki ni nujno pomemben, lahko pa nakazuje na morebitni problem, ki se bo še zgodil. Informacija je dogodek, ki je zgolj informativne narave. Opisuje na primer uspešno delovanje aplikacije, gonilnikov oz. storitve.

- Sistemski dogodki
  Tudi tu velja podobna delitev dogodkov kot pri aplikacijskih dogodkih, s to razliko, da so dogodki sistemskega izvora.

- Varnosti dogodki
  Običajno je ta tip dogodkov najbolj zanimiv za nadaljnjo obravnavo in forenzično analizo. Dogodek ima lahko le dve stanji – lahko je uspešen ali neuspešen. Primer takih dogodkov so: prijava uporabnika v sistem, dostop do vira v skupni rabi idr.

Različica OS Windows 7 vsebuje še dva dodatna dnevnika: namestitveni in posredovani dnevnik. V slednjem se nahajajo posredovani dnevniški zapisi iz drugih računalnikov. Namestitveni dnevnik vsebuje podrobnejše informacije o nameščenih in odstranjenih aplikacijah.

Znano je, da Windows OS nimajo standardnega protokola za transport dnevnikov [11] tako kot ga ima Linux OS. Slednji uporablja syslog protokol. Problem postane še večji, ko moramo analizirati domenske prijave uporabnikov. Predpostavimo, da uporabljamo Windows domenski kontroler, kjer se prijave beležijo v varnostni dnevnik. Če je domenskih kontrolerjev več, pomeni, da moramo pregledati vse. Postopek je zamuden in nepregleden. V tem primeru se nam zdi centralizacija dnevnikov edina prava rešitev. Skupina zanesenjakov je izdelala odprtokodno rešitev, ki rešuje problem transporta Windows dnevnikov. Gre za projekt LASSO. Aplikacija zna zajeti dnevnike OS Windows in jih posredovati syslog strežniku ali sistemu SIEM.

Aplikacije

Pri aplikacijah je nabor še pestrejši: protivirusni sistem, podatkovne baze, poštni sistem, spletne aplikacije, interne aplikacije idr. V splošnem nas zanimajo vse pomembnejše oz. ključne aplikacije v IS. Še posebej nas zanimajo dogodki kot so:

- zagon/zaustavitev aplikacije,
- sprememba privilegijev,
- nedosegljivost storitve,
- poslabšanje performanc idr.

Primer. Dnevnike centralnega protivirusnega sistema lahko uporabimo za alarmiranje v primeru nenadnega povečanega števila okužb ali v primeru nedelovanja posodobitve protivirusnih definicij.

Beleženje in zajem vseh dogodkov v IS ima lahko za negativno posledico zmanjšanje performanc. Po drugi strani pa s takim načinom dela delujemo proaktivno. Z uporabo tehnike rudarjenja lahko iščemo določene vzorce vedenja in jih analiziramo. Vzemimo primer uporabnika, ki za opravljanje svojega dela običajno dostopa do petih različnih virov (A,B,C,D in E). Opažamo, da se ta vzorec ne spreminja skozi čas. Temu stanju pravimo osnovno stanje (angl. baseline). Vsako odstopanje od osnovnega stanja predstavlja alarm. To bi pomenilo, da je uporabnik nenadoma dostopal do šestega vira (F). Taka opozorila oz. alarme je potrebno raziskati in najti vzrok zakaj je prišlo do tega. Obstaja možnost, da je uporabnik dobil nove zadolžitve in je posledično dostopal do novega vira. Mogoče pa gre za krajo podatkov, ker je uporabnik v odpovednem postopku.

Pri upravljanju dogodkov velja naslednje dejstvo, da če nečesa ne beležiš, tudi ne veš kaj se v sistemu dogaja.

5.5 Namestitev

V predhodnih poglavjih smo se seznanili na kaj vse je potrebno pomisliti preden se odločimo za nakup sistema SIEM. Postavitev takega sistema lahko traja od nekaj mesecev, v redkih primerih pa celo nekaj let. Vse je odvisno od zastavljenih ciljev in angažiranosti projektne skupine.

V nadaljevanju bomo našteli nekaj dejavnikov, ki pripomorejo k skrajšanju časa postavitve. Prvi dejavnik, ki bistveno pripomore k krajši implementaciji, je zajem dnevnikov z namensko napravo, torej brez agentov. Nameščanje in prilagajanje agentov je zamudno opravilo. Medtem ko v primeru namenske naprave konfiguracijo opravimo centralno in to za večjo množico dnevnikov oz. naprav. Namestitveni čarovniki še dodatno olajšajo delo. Pri postavitvi je zaželena pomoč zunanjega izvajalca. Slednje je predmet pogodbe.

Naslednji pomemben dejavnik predstavlja poznavanje omrežja in njegova dokumentacija. Tu so še ostali dejavniki, ki dodatno pripomorejo k hitrejši postavitvi:

- uporaba obstoječega podatkovnega centra za hrambo dnevnikov,
- predpripravljena poročila,
- predpripravljeni osnovni filtri in pravila za nadaljnje alarmiranje incidentov,
- naklonjenost in predanost vseh članov projekta.

Po končani postavitvi sistema SIEM nastopi faza učenja in postopne optimizacije sistema (angl. tuning). Optimizacija je del procesa izboljšave storitve in lahko traja tudi nekaj let. ITIL metodologija zagovarja stališče, da mora biti proces optimizacije stalno prisoten. Ta proces nenehnega izboljševanja storitev je podrobneje opisan v peti ITIL knjigi (Continual Service Improvement).

V poglavju 6.5 bomo predstavili končno postavitev izbrane rešitve.

5.6 Najbolj pogoste napake

V nadaljevanju se bomo seznanili z najbolj pogostimi napakami, ki se dogajajo pri implementaciji sistema SIEM [4].

Prva v nizu najbolj pogostih napak je, da **dogodkov sploh ne beležimo**. Določeni sistemi oz. aplikacije imajo že privzeto vključen nivo beleženja dnevnikov. Medtem ko nekateri sistemi (Oracle baza, Microsoft SQL idr.) tega nimajo in je potrebno ročno vključiti generiranje dnevniških zapisov.

Dnevnike beležimo, ampak jih ne spremljamo
SIEM ni rešitev za vse naše težave, temveč je le orodje, ki nam olajša vsakodnevno pregledovanje dnevnikov. Torej brez spremljanja dogajanja v realnem času nam dnevniki ne koristijo. Slednje ne velja, če SIEM uporabljamo samo za zagotavljanje skladnosti. Tu nastopi vprašanje smiselnosti naložbe in morebiten pomislek o uporabi prosto dostopnih SIEM rešitev.

Prekratek čas hranjenja dnevnikov
Da bi se izognili omenjeni težavi, je potrebno v zgodnji fazi implementacije, predvideti ustrezno količino prostora za hrambo dnevnikov. Diskovni prostor je relativno poceni, ampak še vedno obstajajo določene omejitve znotraj sistemov SIEM. Prvi nivo hrambe dnevnikov je običajno na namenski napravi oz. centralnem SIEM strežniku. Ta je omejen s številom diskov, ki jih je mogoče vgraditi v strežnik. Drugi nivo hrambe predstavlja zunanje diskovno polje in je namenjeno trajnejši hrambi dnevnikov. Pogostokrat je odločitev koliko časa potrebujemo določene dnevnike odvisna od določene regulative.

Določanje prioritete dnevniškega zapisa pred zajemom
Tu nastopi vprašanje katere naprave vključiti v zajem in katere prezreti. Kaj hitro se nam lahko zgodi, da smo določenim sistemom dali prednost (višjo prioriteto). Npr. IDS/IPS sistemi imajo običajno višjo prioriteto kot VPN koncentratorji. Iz slednjega sklepamo, da je zunanja grožnja pomembnejša od notranje. V primeru, ko moramo raziskati notranjo goljufijo ali napad, so VPN dnevniki nepogrešljivi del uganke. Da bi se izognili tej napaki Chuvakin predlaga [4], da v začetni fazi implementacije beležimo vse. Kasneje pa na podlagi opažanj in izkušenj prilagodimo prioriteto določenim napravam.

Ignoriranje aplikacijskih dnevnikov
Pogostokrat se daje prednost dnevnikom omrežne opreme pred aplikacijskimi dnevniki. Povod za to napako je nerazumevanje pomembnosti aplikacijskih dnevnikov. Nemalokrat so te aplikacije ključne za poslovanje organizacije in zato je še toliko bolj pomembno, da jih vključimo v SIEM. Običajno imajo aplikacije svoj format beleženja, ki ga SIEM ne razume, ampak je zato potrebno prilagoditi agenta. Določene aplikacije pa sploh nimajo možnosti generiranja dnevnikov. V takih primerih se lahko le obrnemo na proizvajalca programske opreme in podamo zahtevek za spremembo (angl. request for change).

Spremljanje samo znanih dogodkov
V začetni fazi implementacije je najlažje iskati dogodke, ki jih poznamo. Bodisi so to dobri (nevtralni) ali slabi (škodljivi) dogodki. Običajno je za slednje več zanimanja in prej pritegnejo našo pozornost. Tudi sam SIEM vsebuje že predpripravljene akcije oz. alarme v primeru napada. Sistemi SIEM s časom postaja vse zrelejši produkt na področju varnosti. Nekateri proizvajalci so že vgradili sistem za podatkovno rudarjenje (angl. data mining). Ta pristop nam omogoča odkrivanje novih anomalij v IS.

6. Odločitveni model

Pred nami je odločitveni problem. Kateri SIEM produkt izbrati? Problem bomo rešili oz. zastavljene cilje dosegli z izborom ene izmed nabora rešitev (v nadaljevanju različic). Izbora najustreznejše različice se bomo lotili sistematično z uporabo metode večparametrskega ali večkriterijskega odločanja (poglavje 6.3). Ker je ponudba sistemov SIEM preširoka za zajetje vseh petindvajsetih ponudnikov [27], smo v podrobnejšo analizo odločanja zajeli naslednje tri ponudnike: ArcSight, RSA (EMC) in CA. Z vsakim posebej smo izvedli trimesečno testno postavitev, kar je še dodatno pripomoglo h kvalitetnejši končni odločitvi.

V tem poglavju opisan postopek odločanja je zasnovan tako, da je ponovljiv in uporaben tudi za druga podjetja. Ne glede na izbrane tri ponudnike lahko odločevalec izbere poljubne ponudnike in uporabi opisano metodologijo.

Za pomoč pri začetni izbiri SIEM ponudnikov, lahko uporabimo Gartnerjevo analizo SIEM produktov, ki je predstavljena v poglavju 6.6. Slednja zajema ocenjevanje petnajstih SIEM produktov glede na izbrane kritične zmogljivosti in tipe postavitev.

V nadaljevanju sledi nekaj definicij osnovnih pojmov po knjigi Odločanje in modeli [2].
Odločanje je proces, v okviru katerega izbiramo ali ocenjujemo različice z namenom, doseči določene cilje. Običajno izbiramo med večjim številom različic, ki se med seboj izključujejo.

Odločevalec ima v procesu odločanja glavno vlogo. Na začetku postopka opredeli cilje, različice in kriterije. Sledi primerjava in analiza izbranih lastnosti različic ter potrditev zmožnosti doseganja ciljev. Ko je ta faza zaključena, odločevalec sprejme **odločitev** in izbere eno izmed različic ali pa jih zanemari. Odločitev je zavestna in običajno nepovratna dodelitev virov. Posledice odločitve se kažejo v boljšem ali slabšem doseganju zastavljenih ciljev.

Različice predstavljajo različne izbire, ki jih imamo na voljo pri odločanju. Poleg omenjenih se uporabljajo še drugi izrazi: alternative, variante ali možnosti.

Na podlagi **kriterijev** primerjamo, vrednotimo in izbiramo različice glede na cilje odločevalca. Poleg omenjenega termina se uporabljajo še drugi izrazi: sodila in lastnosti različic.

Parameter je lastnost, ki jo opazujemo pri različicah in lahko vpliva na oceno njegove kakovosti ali zaželenosti. Primer parametra bi bila cena.

Z **Atributom** ali merilom označujemo parameter, ki ima definirano mersko lestvico (npr. cena izražena v evrih).

Odločitveni proces
Je proces sistematičnega zbiranja in urejanja znanja. V tem procesu naj bi pridobili dovolj informacij za ustrezno odločitev in s tem zmanjšali možnost napačne izbire ter se tako izognili negativnim posledicam. Želja vsakega odločevalca je, da bi proces potekal hitro in ekonomično, odločitev pa naj bi bila čim boljša.

Odločanje je v splošnem večfazni proces. To pomeni, da ne zajema samo odločitve o izbiri različice, ampak tudi vse aktivnosti, ki potekajo pred njeno izbiro in po njej. Pred izbiro so to navadno aktivnosti povezane s preučevanjem odločitvenega problema, definiranjem ciljev, zbiranjem informacij o različicah in oblikovanjem kriterijev. Bohanec navaja, da odločitvena analiza predlaga sistematičen pristop k reševanju odločitvenih problemov.

Odločitveni proces je razdeljen na pet faz (slika 13), v okviru katerih potekajo naslednje aktivnosti [2]:

- strukturiranje in razgradnja odločitvenega problema na manjše in lažje obvladljive podprobleme,
- analiza dostopne informacije o odločitvenem problemu, podatki o alternativah ter analiza negotovosti in tveganja ob upoštevanju preferenc odločevalca,
- uporaba vseh teh informacij za optimalno oz. vsaj čim boljše doseganje ciljev odločanja.

Faza 1: Prva faza se prične, ko želimo rešiti odločitveni problem, ki je dovolj zahteven, da ga je smiselno reševati na sistematičen in organiziran način. V tej fazi poskušamo čim bolje spoznati, razumeti in definirati problem. Oblikuje se odločitvena skupina z odločevalcem v glavni vlogi. Pri zahtevnejših problemih je potrebno razmisliti tudi o morebitni vključitvi strokovnjakov, svetovalcev, odločitvenih organov in moderatorjev ter drugih predstavnikov povezanih z odločitvijo. Ti si postavijo cilje, ki jih želijo doseči z odločitvijo. Običajno se že v tej fazi določi okviren potek nadaljnjih faz.

Odločili smo se, da bomo prvo fazo odločitvenega procesa dopolnili s SWOT analizo. V naslednjem poglavju bomo najprej analizirali kako danes upravljamo z varnostnimi informacijami in dogodki in nato opravili še SWOT analizo v primeru, če se odločimo za postavitev sistema SIEM.

Faza 2: V fazi prepoznavanja različic se je potrebno vprašati, katere so tiste različice, med katerimi lahko izbiramo. Običajno je želja prepoznati in definirati čim več različic, saj to vodi v večje možnosti, da bomo izpolnili zastavljene cilje. Pri iskanju različic si pomagamo na več načinov: razpis, splet, rezultati testov, priporočila, lastne preference idr. V nekaterih primerih se lahko prepoznava oz. dodajanje novih različic izvede za modeliranjem (za fazo 3). Slednje pride v poštev takrat, ko razvijamo večparametrske odločitvene modele, ki so načeloma neodvisni od posameznih različic. V tem primeru lahko različice definiramo šele zatem, ko je model že razvit. Priporočljivo je, da med različice vključimo tudi možnost, da se sploh ne odločimo.

Faza 3: Ta faza je ena najbolj značilnih, saj tu nastopi izgradnja modela. Z njim nato ovrednotimo različice, jih primerjamo med sabo, ocenimo tveganja in opravimo različne druge izračune. V splošnem gre za matematične ali grafične modele, s katerimi lahko opišemo in opredelimo najpomembnejše komponente odločitvenega problema:

a) struktura odločitvenega problema – tu se vprašamo ali je mogoče odločitveni problem razgraditi na manjše in po možnosti lažje obvladljive odločitvene podprobleme,
b) kriteriji – v modelu opredelimo kriterije, ki jih je potrebno upoštevati pri vrednotenju in izbiri različic,
c) preference – so v testni povezavi s kriteriji, saj izražajo subjektivno mnenje odločevalca o tem katere različice so bolj zaželene, oz. katere so pomembnejše od drugih,

d) negotovosti – prepoznati moramo kateri so tisti pojavi, procesi ali aktivnosti, ki jih ni mogoče nadzorovati, vendar lahko bistveno vplivajo na končno odločitev.

Faza 4: V tej fazi vrednotimo različice s pomočjo izdelanega modela. Na ta način dobimo za vsako različico neko oceno kvalitete oz. koristnosti glede na zastavljene cilje odločitvenega problema. Ob tem običajno ocenimo tudi tveganje pri izbiri različice. Na osnovi teh izračunov lahko različice uredimo od najboljše do najslabše. Pri izbiri so nam v pomoč različne tehnike oz. analize: analiza kaj-če, analiza občutljivosti, simulacija Monte Carlo in selektivna analiza.

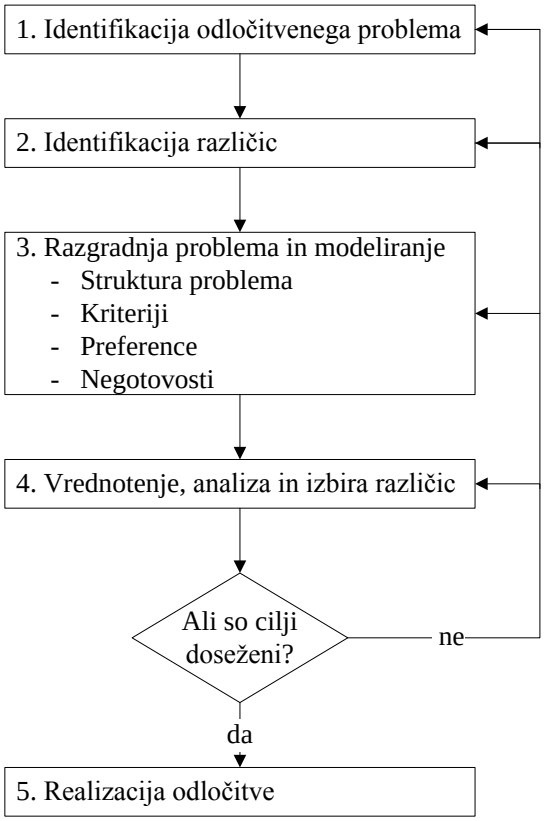
V procesu odločanja se odločevalec pogosto vrača nazaj na predhodne faze, tako da odločanje izvede kot iterativni proces. Na koncu izberemo različico z najvišjo koristnostjo in še sprejemljivim tveganjem. Ker je proces izbire zaključen, lahko začnemo z uresničevanjem odločitve.

Faza 5: Ta faza je rezultat celotnega odločitvenega procesa. V prejšnji fazi smo se odločili za različico, sedaj jo je potrebno realizirati. To pomeni, da začnemo dodeljevati sredstva za uresničitev izbrane različice in da je ta proces v splošnem nepovraten.

Ob zaključku odločitvenega procesa se nam poraja naslednje vprašanje: kako vemo, da smo se prav odločili? Gre za vprašanje kakovosti odločitve, ki je eno najtežjih vprašanj pri odločanju. Težava je v tem, da lahko različice nepristransko ovrednotimo. Druga težava nastane zaradi subjektivnosti odločitve. Odločevalec ima lahko drugačne poglede na preference in kriterije, kot npr. nek drug odločevalec. Kar je za nekoga dobra odločitev, lahko za drugega predstavlja pravi polom. Presojanje kakovosti odločitve zato nikdar ni popolnoma objektivno, saj pri tem vedno nastopajo subjektivni dejavniki.

Kakovost odločitve lahko torej ocenimo le posredno. Najpogosteje nas zanimajo naslednji vidiki:

- kakovost izbrane različice,
- kakovost odločitvenega procesa,
- kakovost realizacije odločitve.



Slika 13: Faze odločitvenega procesa

6.1 Identifikacija odločitvenega problema

V nadaljevanju bomo SWOT analizo prilagodili našim potrebam. Namen naloge je izdelati odločitveni model postavitve sistema SIEM. Pred odločitvijo je potrebno analizirati trenutno stanje in sicer kako danes upravljamo z varnostnimi informacijami in dogodki.

SWOT analiza je analiza prednosti, slabosti, priložnosti in nevarnosti (angl. strengths, weaknesses, opportunities, threats v nadaljevanju SWOT). Gre za eno najbolj pogosto uporabljenih analiz v sklopu poslovnih ved [10]. Spada v proces strateškega načrtovanja. Načrtovanja je lahko usmerjeno na organizacijo kot celoto ali pa na posamezne sklope znotraj organizacije (procese, storitve, produkte idr.).

Prednosti se kažejo kot zmožnosti oz. sposobnosti podjetja, da doseže določene cilje. Slabosti so tiste aktivnosti podjetja, ki lahko ovirajo ali zadržujejo doseganje opredeljenih ciljev. Priložnosti so razmere v zunanjem okolju. Z njihovo pravilno in natančno uporabo ima podjetje možnost, da doseže svoje cilje. Nevarnosti pa predstavljajo tisti dejavniki v okolju, ki lahko ogrozijo doseganje želenih ciljev in na katere podjetje nima veliko vpliva.

Na SWOT analizo vplivajo naslednji dejavniki:

a) Notranji dejavniki
   Med notranje dejavnike uvrščamo **prednosti** in **slabosti**. Pri notranjih dejavnikih smo v območju lastnega vpliva, kar pomeni, da se mogoče določene prilagoditve, spremembe oz. kateri drugi ukrepi.
b) Zunanji dejavniki

Priložnosti in **nevarnosti** pa spadata v skupino zunanjih dejavnikov oz. dejavnikov iz okolja. Zunanji dejavniki imajo lastnost, da nanje ne moremo vplivati. Preprosto jih moramo sprejeti in se jim prilagoditi.

Analiza notranjih in zunanjih dejavnikov ima še večjo uporabno vrednost, če dobljena spoznanja preslikamo v strategije. Pomembno je, da jih oblikujemo tako, da prednosti izkoristimo, slabosti odstranimo, ter razvijemo strategijo v smeri prihodnjega izrabljanja priložnosti in izogibanja nevarnostim. Vse ugotovitve lahko učinkovito prikažemo v t.i. SWOT matriki (tabela 5).

Notranji dejavniki / Zunanji dejavniki	**PREDNOSTI (S)**	**SLABOSTI (W)**
PRILOŽNOSTI (O)	**SO strategije** Strategije, ki poskušajo uporabiti prednosti za izkoriščanje priložnosti	**WO strategije** Strategije, ki poskušajo izkoristiti priložnosti s premagovanjem slabosti
NEVARNOSTI (T)	**ST strategije** Strategije, ki uporabljajo prednosti za izogibanje nevarnostim	**WT strategije** Strategije, ki minimizirajo slabosti in se izogibajo nevarnostim

Tabela 5: Prikaz SWOT matrike

6.1.1 Analiza stanja

Podjetje nima implementiranega centralnega upravljanja dnevnikov oz. dogodkov. Edina izjema je syslog strežnik, ki ima funkcijo zbiranja dnevniških zapisov izključno omrežnih naprav. Pregledovanje dnevnikov posamezne storitve oz. sistema je omejeno v skladu z varnostno politiko podjetja in pooblastili skrbnika. Slednje bi v praksi pomenilo, da skrbnik sporočilnega sistema (npr. Microsoft Exchange) dnevno pregleda dnevnike na vseh strežnikih, ki so del sporočilnega sistema. Delo je sila zamudno, saj se je potrebno na vsak strežnik prijaviti in ročno pregledati vse dnevnike (varnostne, sistemske in aplikacijske).

Naslednja težava je v tem, da skrbniki nimajo celotnega pogleda nad dogajanjem v IS in s težavo nadzorujejo učinkovitost varnostnih ukrepov in ustrezno informacijsko varnost. IS ima določene varnostne rešitve, ki pa med seboj niso povezane.

IS podjetja je čedalje bolj kompleksno okolje. Lokacijska razpršenost je še dodatno zvišala nivo kompleksnosti. V IS so bile vpeljane določene varnostne rešitve (IDS/IPS, 802.1x, segmentacija omrežja idr.) z namenom zagotavljanja višje stopnje informacijske varnosti.

Najpogostejše težave, s katerimi se skrbniki posameznega sistema soočajo, so:
- dolgotrajno pregledovanje, urejanje in razumevanje dnevniških zapisov,
- ogromna količina dogodkov onemogoča pravočasni odziv na anomalije,
- ročno reševanje incidentov vodi v slabo učinkovitost in nesistematično ukrepanje,
- ne obstaja postopek alarmiranja,
- koreliranje dogodkov je ročno in v večini primerov neučinkovito,
- otežena izdelava poročil in nagnjenost k napakam,
- različni formati dnevniških zapisov še dodatno otežuje pregledovanje,

- razpršenost podatkov oz. obstoječih varnostnih sistemov,
- nove varnostne grožnje, porast notranjih groženj in zlorab,
- preobremenjenost skrbnikov.

V tabeli 6 so prikazane vse štiri aktivnosti, ki se nanašajo na uvedbo sistema SIEM.

PREDNOSTI	SLABOSTI
- centralizirano upravljanje dnevnikov - enotna hramba dnevnikov (ena PB) - izdelava poročil o skladnosti - obvladovanje groženj - hitrejše in učinkovitejše alarmiranje - izdelava korelacij - celovitejši pregled nad delovanjem IS - možnost povezovanja z novimi sistemi - upravljanje varnostnih dogodkov - spremljanje uporabnikov - povezava AD in Oracle uporabnikov - spremljanje podatkov - spremljanje aplikacij - izboljšanje doslednosti pri izpolnjevanju internih varnostnih politik	- slabo poznavanje SIEM tehnologije - slabo poznavanje omrežja - pomanjkanje usposobljenega kadra - nenaklonjenost skrbnikov novemu sistemu - prezaposlenost SIEM skrbnikov - začasna manjša delovna produktivnost ostalih udeležencev - nameščanje agentov za zajem dogodkov
PRILOŽNOSTI	**NEVARNOSTI**
- zvišanje stopnje varnosti pred napadi - konkurenčna prednost - hitrejše in pravilnejše odločanje - pravočasne in točnejše informacije - zagotavljanje skladnosti - boljši pregled nad delovanjem IS - možnost širitve funkcionalnosti sistema SIEM - hitrejši odziv na nenehne spremembe	- pomanjkanje finančnih virov - slabe performance zajema dnevnikov (zaradi razpršenosti naprav po omrežju) - poslabšanje performanc v primeru povečanja količine dogodkov - nekritična uporaba sistema in preveliko zanašanje na odgovore, ki jih sistem ponuja - ranljivost sistema v fazi postavitve - poenostavljanje rešitev - slaba podpora - sprememba zakonodaje (npr.: Zakon o bančništvu)

Tabela 6: SWOT analiza za uvedbo sistema SIEM

Splošni namen SWOT analize je predstaviti vse štiri aktivnosti tako, da bo podjetje po najboljšim močeh gradilo na prednostih, ki jih nudi uvedba sistema SIEM. Izboljšalo oz. celo odpravilo področja kjer se pojavljajo slabosti, izkoristilo vse priložnosti, ki se porajajo ob uvedbi in se čim bolje prilagodilo oz. izognilo nevarnostim.

6.1.2 Zrelost procesov

V poglavju 2.3 smo si pogledali kakšna so priporoča ITIL glede upravljanja dogodkov in upravljanja incidentov. Sledi njun opis zrelosti procesov.

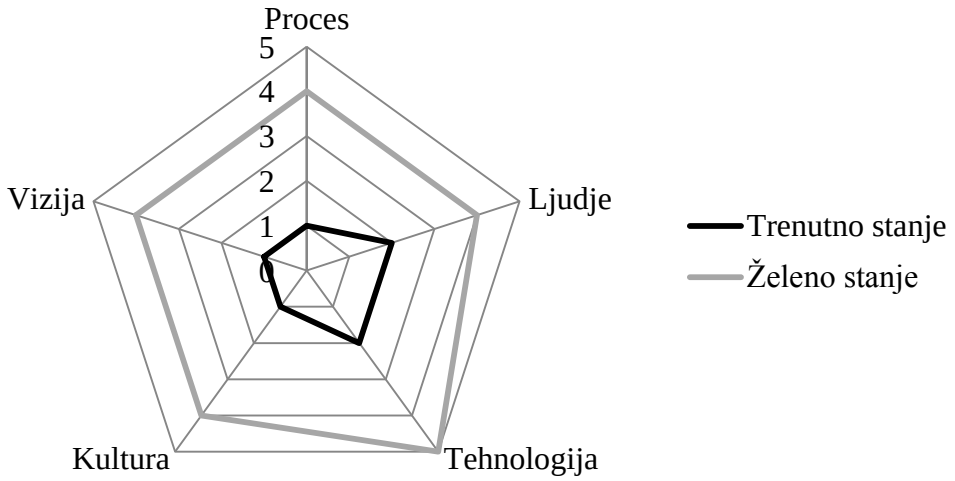
Za analizo zrelosti obeh procesov bomo uporabili zrelostni model procesov upravljanja storitev (angl. Process Maturity Framework, krat. PMF). Ocenili bomo razkorak med trenutnim in želenim stanjem za naslednja področja: proces, ljudje, tehnologija, kultura in vizija. Sam proces lahko doseže enega od petih nivojev: začetni, ponovljiv, definiran, upravljan in optimiziran [9].

Upravljanje dogodkov
Celoten **proces** upravljanja dogodkov je v začetni fazi. Aktivnosti se izvajajo ad-hoc oz. po potrebi. Podjetje nima točno definiranega procesa upravljanja dogodkov. Aktivnosti se izvajajo naključno, običajno le takrat, ko nastopi težava.

Ljudje in **tehnologija** sta edina na drugem nivoju (ti. ponovljiv nivo). Vloge so definirane do te mere, da vsak skrbnik ve katere sisteme mora pregledovati oz. spremljati. Prisotna so določena orodja, ki skrbniku olajšajo delo. Manjka pa kontrola nad izvajanjem in centralna baza podatkov.

Kultura je zgolj orientirana na posamezna orodja in tehnologijo.
Dejstvo je, da je bilo to področje zapostavljeno tako s stališča zagotovljenih denarnih sredstev kot procesno. Dvig nivoja **vizije** je nujen.

Želimo, da proces postane vsaj definiran, če že ne upravljan. Torej v prvi fazi je potrebno zagotoviti ustrezna sredstva za nakup orodja (SIEM produkt; izbor ponudnika bo opisan v nadaljevanju). Nato je potrebno definirati celoten proces in aktivnosti znotraj upravljanja dogodkov (glej sliko 7). Za tem pride vzpostavitev sistema in določitev vlog (poglavje 5).



Slika 14: Zrelost procesa upravljanja dogodkov

Upravljanje incidentov
Podjetje ima implementirano orodje Service Desk Manager (v nadaljevanju SDM), rešitev podjetja CA Technologies. SDM ima definirani dve glavni nalogi:

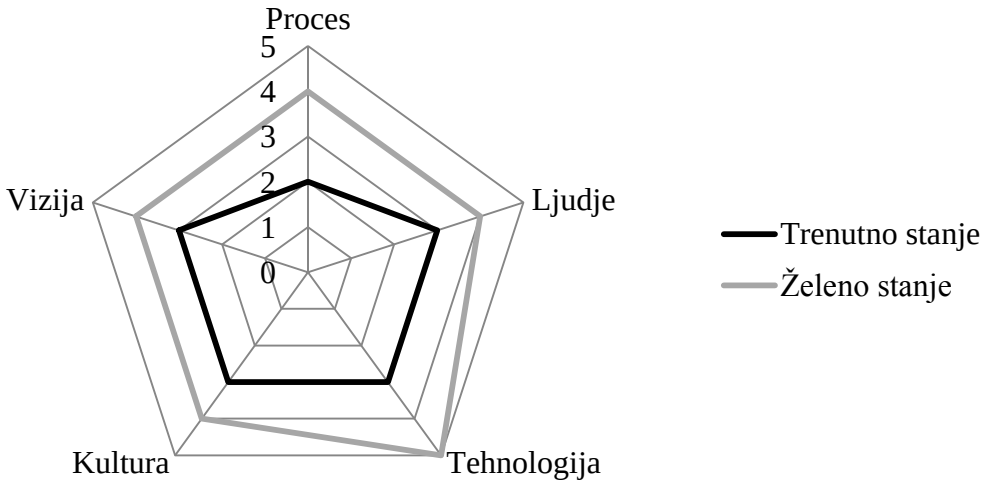
a) Enotna točka dostopa za pomoč uporabnikom (ti. storitveni center)
b) Skrbi za izvajanje procesa upravljanja incidentov

Proces je definiran in večinoma reaktiven. Problem se pojavi že v samem začetku procesa – pri zaznavi incidentov. Manjka zaznava incidentov iz drugih sistemov, kot npr. sistem za upravljanje dogodkov. Proces je definiran le za tiste incidente, ki so bili oddani preko storitvenega centra in majhen nabor infrastrukturnih strežnikov. Posledično je proces najslabše ocenjen (ponovljiv).

Ljudje in **tehnologija** sta na tretjem nivoju (opredeljena). Razlog je v dveletni uporabi orodja SDM. V tem času so se dokončno izoblikovale vloge in zadolžitve posameznikov. Definirani

sta tudi dve stopnji podpore ter funkcionalna in hierarhična eskalacija. Orodje omogoča kvalitetno analizo in izdelavo poročil, saj se podatki shranjuje v centralno bazo podatkov.

Kultura je storitveno in uporabniško orientirana s formaliziranim pristopom.
V sklopu **vizije** so cilji dogovorjeni in dokumentirani. Poročila se redno analizirajo in pregledujejo.



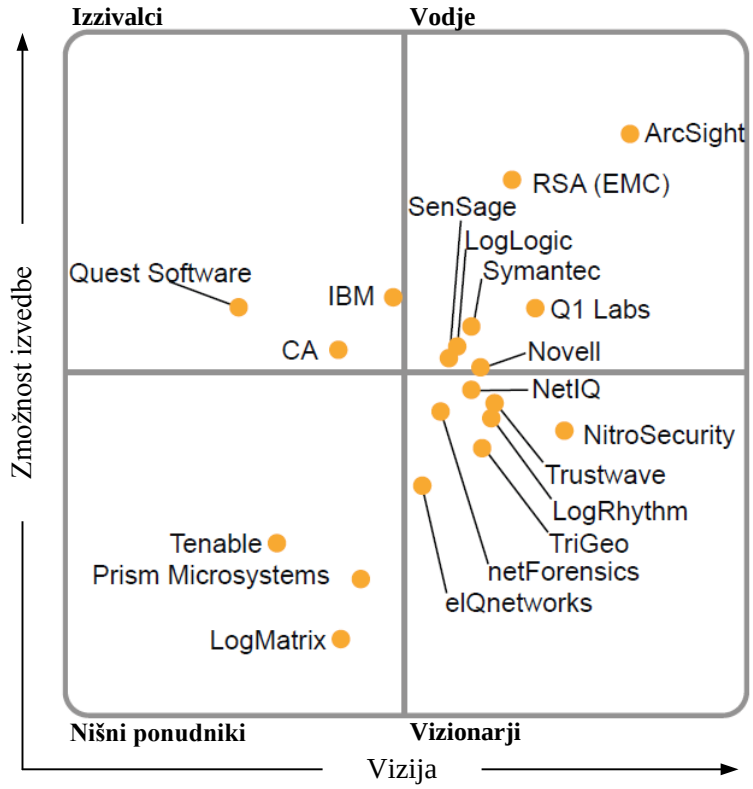
Slika 15: Zrelost procesa upravljanja incidentov

6.2 Identifikacija različic

Analiza trenutnega stanja na področju upravljanja varnostnih informacij in dogodkov jasno nakazuje, da je prenova oz. vzpostavitev procesa upravljanja dogodkov nujno potrebna.

V ta namen je podjetje leta 2010 pristopilo k iskanju morebitne rešitve na področju sistemov SIEM. Kot izhodišče pri iskanju različic smo upoštevali Gartnerjev "magični kvadrant" (angl. magic quadrant) [27]. Slednji je prikazan na sliki 16. Kvadrant odraža Gartnerjevo analizo ponudnikov SIEM orodij glede na dva kriterija [31]. Prvi je zmožnost izvedbe (y-os), ki zajema storitve, splošno stanje, ceno, tržno odzivnost, izvedbo, operacije in uporabnikove izkušnje. Drugi kriterij se osredotoča na vizijo (x-os), ki vsebuje razumevanje trga, poslovni model, inovativnost ter tržno, prodajno, proizvodno in geografsko strategijo.

Kvadrant je razdeljen na štiri dele: vodje, vizionarji, nišni ponudniki ter izzivalci. Vodje obvladujejo večji del trga in imajo veliko število strank. So prodorni in imajo izdelano dolgoletno vizijo. Nišni ponudniki so osredotočeni na ponudbo iz segmenta, ki je značilen za določeno geografsko področje, medtem ko so vizionarji usmerjeni na prihodnost in uporabo nove tehnologije s pomanjkanjem podpore in finančne moči. Izzivalci imajo močan položaj na trgu, vendar zaostajajo za vodji. Razlogi so v pomanjkanju vizionarstva in širjenju trga.



Slika 16: Gartnerjev magični kvadrant ponudnikov SIEM (maj 2010)

V tako imenovanem vodilnem kvadrantu je 7 ponudnikov: ArcSight, RSA (EMC), Q1 Labs, Symantec, LogLogic, SenSage in Novell. Gartner odsvetuje pretirano osredotočenost na vodje in predlaga vključitev ponudnikov iz ostalih področij. Upoštevali smo Gartnerjev nasvet in poleg dveh vodij izbrali še izzivalca (CA):

- ArcSight,
- RSA (EMC),
- CA.

Poleg Gartnerjevega magičnega kvadranta je na izbiro ponudnikov pomembno vplivalo njihovo zastopstvo v Sloveniji in kvalitetno nudenje podpore v fazi postavitve. Z vsemi tremi izvajalci smo se dogovorili za testno postavitev (pilot) v našem okolju.

Tabela 7 prikazuje ponudnikovo SIEM rešitev oz. različico.

Ponudnik		Različica
ArcSight An HP Company	HP/ArcSight	ArcSight
RSA The Security Division of EMC	RSA (EMC)	RSA enVision
ca technologies	CA Technologies	CA Enterprise Log Manager

Tabela 7: Izbrani ponudniki za testno postavitev

6.3 Razgradnja problema in modeliranje

Osnovni odločitveni problem bomo razgraditi na manjše podprobleme ter zgraditi ustrezni odločitveni model. Uporabili bomo večparametrsko metodo odločanja. Glavna značilnost te metode je, da hkrati spremljamo in ocenjujemo več kot le eno lastnost različic. Pri tem za vsakega od parametrov določiti ustrezne kriterije. Zato ta način odločanja imenujemo tudi večkriterijsko odločanje.

Običajno pri takšnem načinu odločanja ne želimo doseči enega samega cilja, kot je npr. upravljanje dnevnikov, ampak več ciljev hkrati. V primeru, da ciljev ni mogoče v celoti izpolniti, se zadovoljimo z delno uspešnostjo. Izvedemo jo lahko le pod pogojem, da skozi celoten proces odločanja strmimo k čim boljšemu izpolnjevanju ciljev.

Metod za podporo večparametrskega odločanja je veliko:
- analiza prednosti in slabosti različic,
- metoda PMI,
- metoda Abacon,
- metoda Kepner-Tregoe,
- uteži parametrov idr.

Za naš odločitveni problem bomo uporabili metodo **uteži parametrov**. Možna sva dva pristopa.
Pristop 1: Najpomembnejšemu parametru določimo neko konstanto (gre za maksimalno vrednost oz. utež, ki je običajno 100). Uteži ostalih parametrov pa potem določimo relativno glede na ta parameter.
Pristop 2: Utež 100 ali 100% razdelimo med vse parametre. Z drugimi besedami uteži določimo tako, da je vsota vseh uteži enaka 100.

Ker je drugi pristop manj prikladen za začetno določanje uteži parametrov, se bomo problema raje lotili s prvim načinom in ga v nadaljevanju normirali na 100 %.

Med obema načinoma predstavitve uteži obstaja preprosta preslikava [2]. Naj bodo $w_1, w_2, \dots, w_n$ poljubne pozitivne uteži, ki jih želimo normirati na 100%. Za vsak parameter k je ustrezna normirana utež ω_k enaka:

$$\omega_k = \frac{100 w_k}{\sum_{i=1}^{n} w_i}$$

Na podlagi zastavljenih ciljev in seznama najpogostejših težav, ki smo jih navedli v analizi (glej poglavje 6.1.1), smo določili naslednje kriterije in pripadajoče uteži:

Kriteriji	**Uteži**	
	Največ 100	Vsota 100
upravljanje dnevnikov in poročanje	100	26%
podpora za upravljanje incidentov	60	16%
namestitev in uporaba	40	11%
spremljanje v realnem času	40	11%
korelacija dogodkov	40	11%

spremljanje aplikacij	40	11%
spremljanje podatkov	20	5%
spremljanje uporabnikov	20	5%
nadzorna plošča	20	5%
skupaj	**380**	**100%**

Tabela 8: Določitev kriterijev in uteži za vrednotenje različic sistema SIEM

Naš glavni cilj je centralno **upravljanje dnevnikov in poročanje**, zato smo temu kriteriju pripisali največjo utež (100). V času pilota bomo še posebej pozorni na zmožnost zajetja dogodkov iz različnih virov (syslog strežnik, IDS/IPS sistema, Windows/UNIX OS, centralne podatkovne baze, protivirusnega sistema, aplikacij, AD idr.). Rešitev mora vsebovati možnost ročnega in avtomatičnega izvajanje tipskih poročil (seznam groženj, seznam kršitev, skladnost s predpisi idr.). Med testiranjem bomo izdelali do petnajst osnovnih varnostnih poročil na osnovi zajetih dnevnikov s pomočjo korelacij.

Podpora za upravljanje incidentov – končna rešitev mora obvezno vsebovati ustrezno podporo za upravljanje incidentov in integracijo z obstoječim orodjem SDM. To je pogoj, če želimo izboljšati proces upravljanja incidentov. Test bo vključeval izvedbo alarmiranje za do deset kritičnih dogodkov z možnostjo nadaljnje povezave na SDM.

Namestitev in uporaba – zaradi pomanjkanja kadra je bistveno, da je rešitev enostavna za uporabo in nadaljnje vzdrževanje. Tudi dodajanje novih funkcionalnosti ne sme biti prevelik izziv za SIEM skrbnike. Preverili bomo tudi možnosti o postavitvi visoko razpoložljive konfiguracije (angl. high availability).

Spremljanje v realnem času – tu bomo primerjali koliko časa potrebuje sistem od dejanskega napada do alarma. Namerno bomo izvedli nekaj tipičnih napadov in beležili čas zaznave.

Korelacija dogodkov – sistem mora vsebovati že predpripravljene osnovne korelacije in imeti možnost izdelave lastnih korelacij. Pozorni bomo tudi na stopnjo zahtevnosti kreiranja novih korelacij.

Spremljanje aplikacij – želja po spremljanju aplikacij kot so: Microsoft Exchange, Microsoft DHCP, Microsoft IIS, ključne lastne aplikacije idr. Večji kot bo nabor aplikacij, ki jih različica podpira, boljša bo ocena.

Spremljanje podatkov – različica mora obvezno omogočati nadzor sistema za upravljanje podatkovnih baz (IBM DB2, Microsoft SQL in Oracle). Preveriti je potrebno, ali vsebuje funkcionalnosti DAM, FIM in DLP. Poudarek bo na DAM in DLP funkcionalnosti.

Spremljanje uporabnikov – želja po spremljanju aktivnosti uporabnikov. Preveri uporabnost te funkcije in nadaljnje možnosti integracije z Windows AD, IdM in HR sistemi.

Nadzorna plošča – želja po pregledni in enostavni nadzorni plošči, ki že na osnovni strani prikaže trenutno "zdravje" sistema.

Obstaja še veliko drugih kriterijev, ki jih lahko vključimo v proces vrednotenja različic sistema SIEM. Pomembno je, da je izbor kriterijev in njihovih uteži prilagojen našim

potrebam. V konkretnem primeru sta glavna cilja vzpostavitev upravljanja dnevnikov in izboljšati proces upravljanja incidentov (skupaj smo jim namenili 42 % celotne ocene).

V nadaljevanju bomo predstavili še druge kriterije, ki jih lahko odločevalec uporabi za svoj konkretni primer odločanja. Osredotočili se bomo na tri najbolj pogoste tipe postavitve sistema SIEM, ki smo jih obravnavali v poglavju 5.1 (zagotavljanje skladnosti, obvladovanje groženj in polna SIEM funkcionalnost).

Cena		
Reference in priporočila		
Bližina izvajalca oz. podpore		
Izkušnje in usposobljenost izvajalca		
Tehnična ustreznost rešitve		
Možnost pogodbenega izvajanja opravil pri zunanjih izvajalcih		
Zagotavljanje skladnosti	**Obvladovanje groženj**	**Polna SIEM funkcionalnost**
Upravljanje dnevnikov in poročanje		Upravljanje dnevnikov in poročanje
	Upravljanje varnostnih dogodkov	Upravljanje varnostnih dogodkov
	Spremljanje podatkov	Spremljanje podatkov
	Spremljanje uporabnikov	Spremljanje uporabnikov
	Spremljanje aplikacij	Spremljanje aplikacij
Namestitev in podpora		Namestitev in podpora
Nadzorna plošča		
Performance		
Čas vzpostavitve		
Diskovne kapacitete		
Možnost nadgradnje sistema		
Podpora oz. integracija s specifično aplikacijo		

Tabela 9: Seznam kriterijev za vrednotenje različic sistema SIEM

Prvih šest kriterijev spada v t.i. osnovne kriterije, ki jih lahko uporabimo pri začetni izbiri ponudnikov. Nato sledijo kriteriji, ki so značilni za določen tip postavitve. Teh šest kriterijev je predlagal Gartner v svoji analizi [30]. Podrobnejša predstavitev Gartnerjeve analize sledi v poglavju 6.6. Zadnjih šest kriterijev lahko odločevalec poljubno uporabi v svojem modelu odločanja.

Na tem mestu velja opozoriti, da lahko preveliko število izbranih kriterij negativno vpliva na celotni proces odločanja. S pretiravanjem lahko zgrešimo bistvo in namen zakaj sploh želimo vzpostaviti sistem SIEM. Zato je ključno, da so kriteriji izbrani premišljeno in da so v skladu z našimi potrebami.

6.4 Vrednotenje, analiza in izbira različic

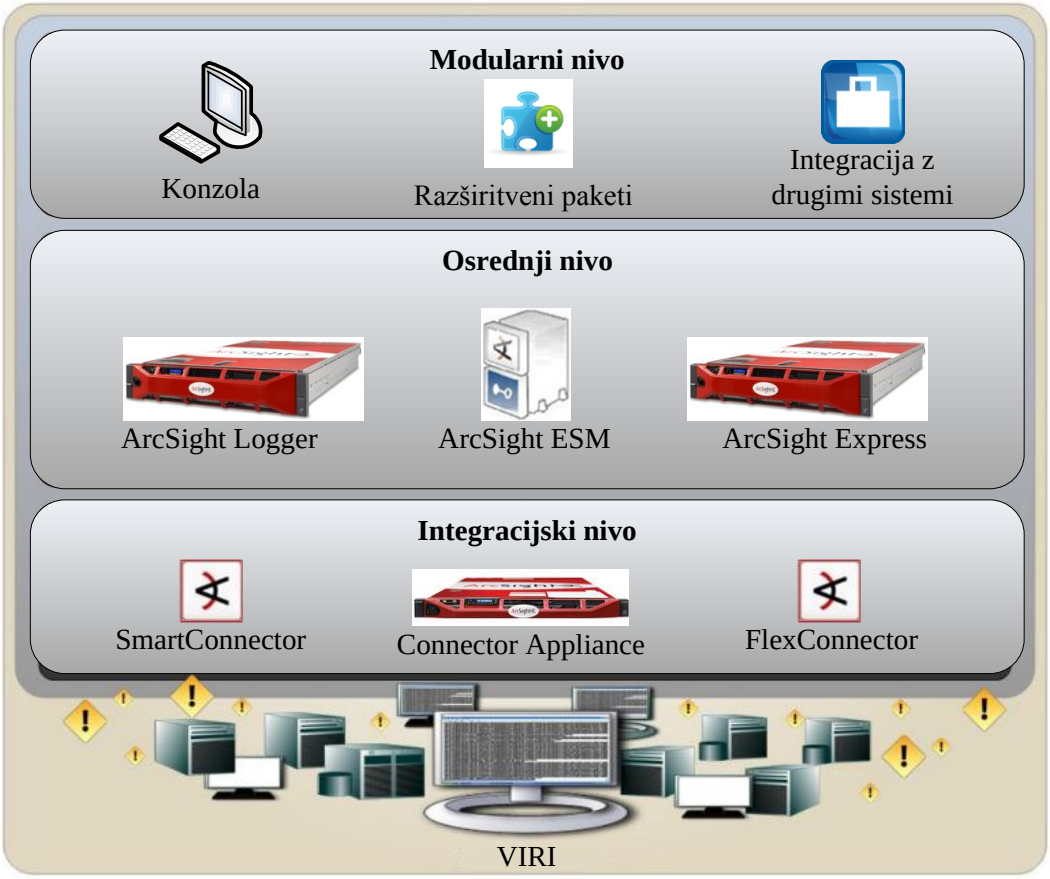
V četrti fazi sledi vrednotenje različic na osnovi izdelanega modela iz prejšnjega poglavja. Kot že rečeno smo se z vsemi tremi izvajalci dogovorili za testno postavitev v našem okolju. Sledi predstavitev različic, arhitekturne rešitve in vrednotenje na podlagi izbranih kriterijev (tabela 8).

6.4.1 ArcSight

Podjetje ArcSight je bilo ustanovljeno leta 2000 v Kaliforniji. Od septembra 2010 podjetje deluje pod okriljem uspešnega podjetja Hewlett-Packard (HP). ArcSight je eno vodilnih ponudnikov SIEM rešitev. Že podatek, da je ArcSight po Gartnerjevih raziskavah že šesto leto zapored vodilni v kategoriji SIEM, pove veliko o uspešnosti podjetja. Poleg tega ima ArcSight po IDC analizah devetnajst odstotni tržni delež v SIEM segmentu.

ArcSight je svoje rešitve zasnoval tako, da so primerne tudi za najbolj kompleksne in geografsko razpršene organizacije z različnimi tehnologijami, proizvajalci in tipi infrastruktur.

ArcSight je zasnoval tristopenjsko arhitekturno rešitev, ki omogoča postavitev različnih scenarijev. S takim pristopom je še lažje izpolniti zahteve naročnika ter mu hkrati omogočiti nadaljnjo razširljivost v skladu z njegovimi potrebami. Slika 17 prikazuje komponente posameznega nivoja. V nadaljevanju si bomo podrobneje pogledali te komponente.



Slika 17: ArcSight arhitekturne komponente

a) Integracijski nivo (Integration Layer)
Najnižji nivo ArcSight rešitve je integracijski nivo, ki zbira dogodke iz različnih virov. Znotraj integracijskega nivoja obstajajo tri ključne komponente: **ArcSight SmartConnector**, **ArcSight FlexConnector** in **ArcSight Connector Appliance**. Skupna naloga omenjenih je zbiranje dogodkov iz različnih virov v njihovi prvotni obliki (tako kot so bili ustvarjeni), ki jih normalizirajo, tako da jih lahko kasneje primerjamo in analiziramo na različne načine.

Connector-ji zbirajo dogodke lokalno in jih preko varne in zanesljive povezave pošiljajo shranjevalnim in korelacijskim komponentam (osrednji nivo).

Ključni pristop ArcSight-a je v normalizaciji vseh dogodkov v poenoten in standardiziran format (CEF). S takim pristopom so mogoče direktne primerjave in analize za različne vire. To nam nudi izredno prilagodljivost in možnost enake analize tudi v primeru, ko zamenjamo tehnologijo (npr. zamenjava omrežne opreme Cisco za Juniper ali Palo Alto).

ArcSight FlexConnector je v bistvu programsko razvojno orodje, ki omogoča izdelavo specifičnega SmartConnector-ja prilagojenega točno določeni napravi, sistemu ali aplikaciji. ArcSight FlexConnector lahko bere in razčlenjuje informacije z drugih naprav in jih preslika v obliko, ki je primerna za nadaljnjo obdelavo in analizo.

Smart Connector-ji so lahko implementirani kot programska oprema na obstoječi infrastrukturi (strežniki, delovne postaje idr.) ali v obliki namenske naprave (ArcSight Connector Appliance). ArcSight je sposoben sprejeti oz. zajeti podatke iz približno 300 različnih naprav, sistemov ali aplikacij. Seznam se nenehno širi in posodablja [29].

b) Osrednji nivo (Core Engine Layer)
ArcSight ESM (Enterprise Security Management) predstavlja glavno komponento celotne SIEM rešitve. Gre za t.i. korelacijsko jedro, ki omogoča podjetju, da ima v realnem času stalen vpogled v varnostne razmere. ESM je na voljo samo v obliki namenske naprave. Omogoča hitro analizo in korelacijo dogodkov v realnem času. Zato je idealna rešitev za odkrivanje, ovrednotenje in ukrepanje proti napadom od zunaj, notranjim grožnjam in kršitvam zahtev o skladnosti. ESM nudi učinkovito zbiranje dogodkov iz širokega nabora naprav v omrežju. Poleg tega omogoča poglobljeno analizo spremljanja uporabnikov, podatkov in aplikacij. Z vgrajenimi koncepti nadzora nad sredstvi in uporabniki, ArcSight ESM omogoča razumevanje kdo je prijavljen v omrežje, katere podatke vidi in katere aktivnosti izvaja. V ESM lahko vključimo vnaprej znane podatke o ranljivosti in kritičnosti posameznih IS, kar omogoča prioritetno obdelavo incidentov v najbolj primernem vrstnem redu. Alarmi kažejo administratorju ključne in najbolj kritične dogodke, na katere se mora podrobneje osredotočiti. ArcSight ESM torej omogoča obsežno in pravočasno izvajanja nadzora, situacijske predstavitve stanja v realnem času, poročanja, analiziranja in vplivanja na izvajanje procesov.

ArcSight Logger so razvili zaradi vse večje potrebe po zbiranju, hranjenju in analiziranju dnevnikov v heterogenih okoljih. Logger je na voljo v obliki namenske naprave ali v obliki programske opreme. Omogoča hitro zbiranje vseh vrst dnevnikov, njihovo hranjenje za poljubna retencijska obdobja, ter zagotavlja ustrezno zaščito. Z zmogljivim orodjem za izdelavo poročil in generiranjem alarmov je lahko samostojna platforma za upravljanje z dnevniki kot tudi dobra osnova za uporabo korelacijskih pristopov in analiz z ArcSight Express ali ArcSight ESM rešitvami.

ArcSight PCI Logger je posebna različica omenjene rešitve za zagotavljanje skladnosti s standardom PCI DSS za organizacije, ki poslujejo s plačilnimi karticami. Naprava PCI Logger zagotavlja varnost podatkov o plačilnih karticah in njihovih lastnikih in s tem tudi skladnost z zahtevami izdajateljev kartic.

ArcSight Express je prilagojena rešitev, ki je namenjena manjšim okoljem in predstavlja manj zmogljiv ArcSight ESM. ArcSight Express omogoča identificiranje pomena nekega dogodka, s tem ko ga vzpostavi v kontekst kaj, kje, kdaj in zakaj se je nek dogodek zgodil. Sprotni alarmi kažejo administratorju najbolj kritične točke v omrežju in širšem sistemu, ki potrebujejo podrobnejši pregled. ArcSight Express je mogoče kupiti le v kombinaciji z ArcSight Logger-jem. Medtem ko lahko Logger deluje samostojno.

ArcSight Express omogoča dokazovanje skladnosti z naslednjimi standardi oz. regulativami: ISO/IEC 27002, SOX, JSOX, NERC, NIST 800-53, PCI DSS, GLBA, FISMA in HIPAA. ArcSight Express ima možnost nadgradnje z modularnim nivojem **ArcSight Compliance Insight Packs**. To so specializirani razširitveni paketi namenjeni izdelavi poročil, ki ustrezajo točno določenim regulativam in standardom.

c) Modularni nivo (Module Layer).

Najvišji nivo ArcSight arhitekture nudi administratorjem in skrbnikom grafični vmesnik za vse ArcSight-ove komponente. Znotraj ArcSight konzole je mogoče določiti posamezne skupine uporabnikov oz. vloge in njihove pravice do posameznih sklopov.

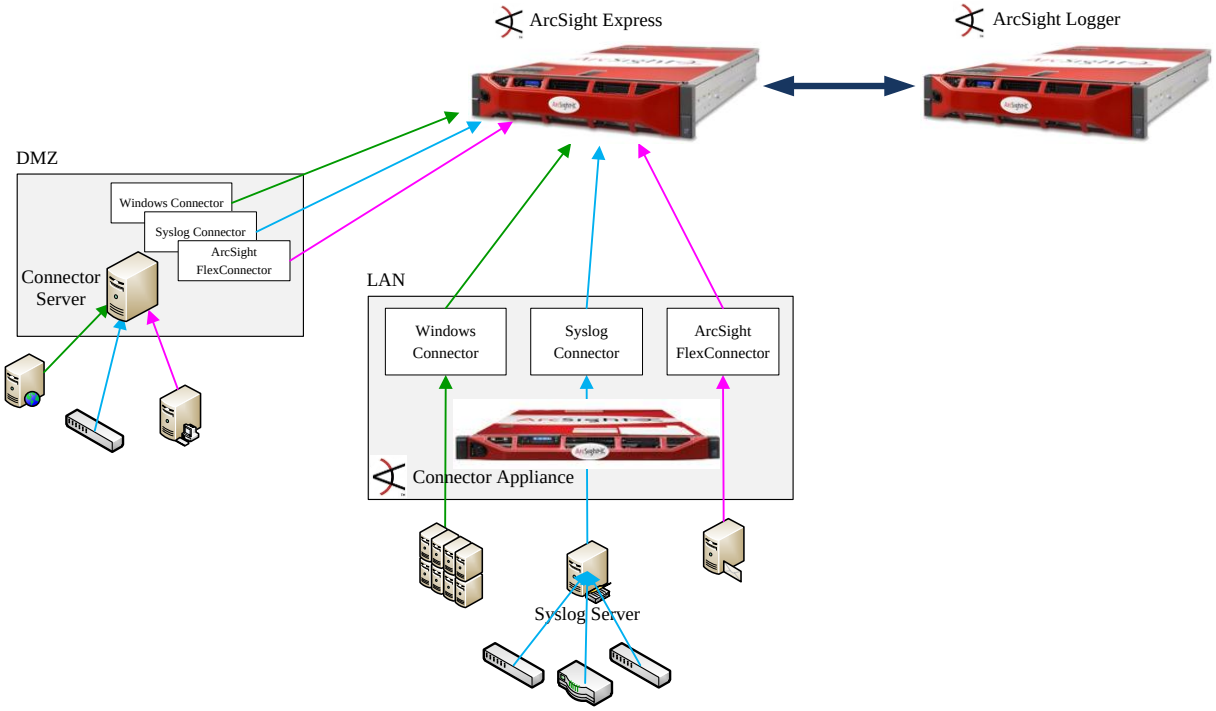
Modularni nivo vključuje tudi razširitvene pakete, ki omogočajo specifičen pogled in upravljanje v skladu z namenom zagotavljanja skladnosti.

ArcSight - TESTNA POSTAVITEV

Glede na analizo stanja, ki smo jo izvedli v poglavju 6.1.1, smo za testne namene uporabili rešitev ArcSight Express (Express + Logger) in ArcSight Connector Appliance. Taka postavitev zmore do 2500 EPS in 750 naprav.

Testna postavitev (slika 18) ponudnika ArcSight je sestavljena iz naslednjih komponent:

- 1x ArcSight Express (M7200-X),
- 1x ArcSight Logger (L3200),
- 1x ArcSight Connector Appliance (C3200),
- 1x Connector server (obstoječi infrastrukturni strežnik).



Slika 18: ArcSight – testna postavitev

Za zajem dnevnikov v lokalnem omrežju (v nadaljevanju LAN) skrbi en Connector Server naprava tipa ArcSight Appliance. Medtem ko smo za zajem dnevnikov iz demilitariziranega območja (angl. demilitarized zone, krat. DMZ) uporabili namenski infrastrukturni strežnik z OS Windows Server 2008 R2, ki ima funkcijo gostitelja Connector server. Tudi omenjeni programski konektor zagotavlja zajem 2500 EPS. Za zajem nepodprtih dogodkov (iz strani ArcSight-a) smo uporabili ArcSight FlexConnector, ki smo ga namestili na Connector Appliance in infrastrukturni strežnik v DMZ. Za vse ostale sisteme in naprave smo uporabili vgrajene konektorje (Windows Connector, Syslog Connector, DNS Connector, AD Connector idr.).

Osnovna ideja je, da vsi konektorji pošiljajo dogodke na osrednjo enoto Express, ta pa jih za tem posreduje v Logger. Logger ima 8 TB diskovne kapacitete in je idealen za daljše hranjenje dogodkov (tudi do pet let). Express ni namenjen trajnemu hranjenju dogodkov, saj premore le 1,6 GB prostora. V primeru da nam diskovne kapacitete na Logger-ju ne zadostujejo, lahko dogodke hranimo na zunanjem diskovnem polju. Ta rešitev je performančno slabša, saj je Logger optimiziran za delo z dnevniki.

Testni sistem je licenciran za 2500 EPS. Med testom se je izkazalo, da je bila ta licenčna omejitev večkrat presežena. Z ustreznimi ukrepi in nastavitvami smo uspeli Connector konfigurirati tako, da Express ni več presegel mejo 2500 dogodkov na sekundo. Mehanizmi združevanja, filtriranja in lokalnega shranjevanja dnevnikov na Connector-jih omogočajo sprotno prilagajanje tudi s stališča pravilne uporabe v okviru licenčnih omejitev. Ponudnik ArcSight zagotavlja, da tudi v primeru krajše prekoračitve števila dogodkov sistem še naprej deluje pravilno.

6.4.2 RSA (EMC)

Ime RSA izhaja iz začetnic treh strokovnjakov (Ron Rivest, Adi Shamir in Len Adleman), ki so leta 1977 opisali RSA algoritem. Spada v družino algoritmov za šifriranje z javnim ključem. Uporablja se v protokolih, ki so namenjeni komunikacijam. RSA velja za varen algoritem le v primeru, da je dolžina ključev dovolj dolga.

Podjetje RSA je bilo ustanovljeno leta 1982 (takrat se je imenovalo RSA Data Security). Od leta 2006 pa RSA spada pod varnostni oddelek podjetja EMC. RSA že tri desetletja uspešno deluje na področju šifriranja in ostalih varnostnih mehanizmov.

RSA je svojo SIEM rešitev poimenoval **enVision**. Na voljo sta dve seriji produktov.

a) enVision ES
   ES rešitve so namenjene arhitekturnim rešitvam z eno napravo. Nadgradnja znotraj serije se izvede le z nadgradnjo licence. Najosnovnejši model zmore do 500 EPS in 100 naprav, najzmogljivejši pa do 7500 EPS in 1250 naprav.

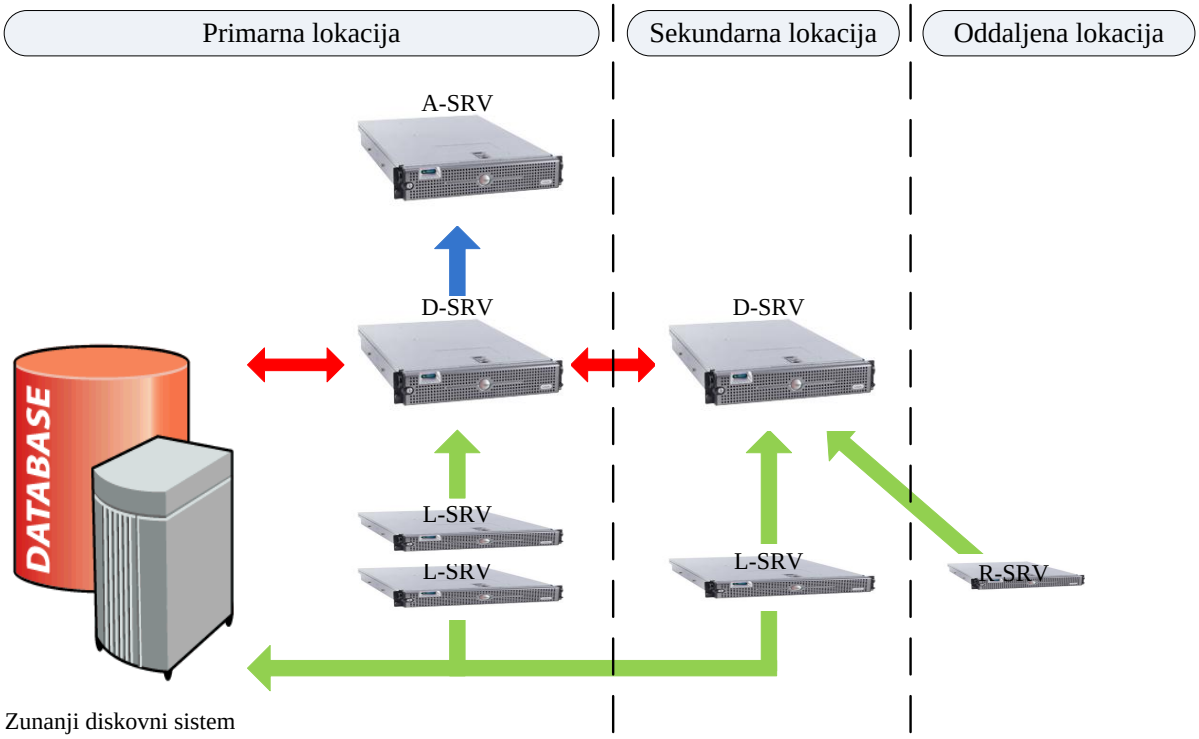
b) enVision LS
   V primeru da bi naš IS generiral več kot 7500 dogodkov na minuto, oz. da bi imeli v upravljanju več kot 1250 naprav, bi morali uporabiti LS linijo. Slednja je namenjena distribuiranim postavitvam. Primer take postavitve je prikazan na sliki 19. LS serijo sestavljajo štiri namenske naprave, ki se med seboj ločijo glede na njihovo funkcionalnost.

   Application server appliance (A-SRV) je strežnik, namenjen analizi in pregledovanju dogodkov. Ko uporabnik sproži poizvedbo v nadzorni plošči, A-SRV ustvari zahtevo in jo pošlje najbližjemu D-SRV. Slednji izvrši želeno poizvedbo ter vrne rezultat.

   Database server appliance (D-SRV) predstavlja napravo za procesiranje dogodkov. D-SRV procesira vsebino L-SRV in R-SRV. V primeru, da imamo več D-SRV instanc, sistem sam poskrbi za medsebojno komunikacijo. Privzeto si D-SRV naprave med seboj izmenjujejo vsebino in znanje enkrat na minuto.

   Local collector appliance (L-SRV) je namenjen zbiranju dogodkov iz omrežnih naprav, sistemov in aplikacij. L-SRV ima dve nalogi: hranjenje originalnih (nespremenjenih) dogodkov in posredovanje normaliziranih in razčlenjenih dogodkov D-SRV. Naprava je dimenzionirana za zajem 5000 do 10000 EPS oz. za 1500 do 2048 naprav. V primeru da naš IS presega omenjene številke, lahko z večanjem števila L-SRV naprav zagotovimo visoko razpoložljivo konfiguracijo.

   Remote collector appliance (R-SRV) je namenjen zbiranju dogodkov za manjša lokacije oz. izpostave. Naprava je dimenzionirana za zajem 1000 do 2000 EPS oz. za 512 do 1024 naprav. Ta zbrane dogodke posreduje D-SRV, saj naprava nima lokalnega diskovja.



Slika 19: RSA – primer LS arhitekture

RSA - TESTNA POSTAVITEV
V testni postavitvi smo implementirali rešitev, ki predvideva le eno napravo iz serije ES. V primeru, da bi se odločili za različico enVision, bi ES serija zadovoljila vse naše potrebe. Uporabili smo model ES 2560, ki zmore do 2500 EPS in 400 naprav. Naprava ima le 300 GB internega spomina, kar je ravno zadoščalo za testne namene. V produkcijski postavitvi je priporočljivo dokupiti zunanje diskovno polje, npr.: Direct Attach Storage Array, Network Attach Storage Array idr.

6.4.3 CA

Podjetje CA Technologies (Computer Associates, v nadaljevanju CA) je bilo ustanovljeno leta 1976. Danes je CA eno največjih proizvajalcev programske opreme in tudi vodilni ponudnik programske opreme za informacijsko varnost. Na področju varnosti velja omeniti protivirusni program eTrust Antivirus in program za zaznavanje in preprečevanje vdorov eTrust Intrusion Detection.

CA je imel leta 2008 na trgu dve SIEM rešitvi: CA Audit in CA Security Command Center (SCC). CA Audit je omogočal osnovni zajem in analizo dnevnikov (SIM funkcionalnosti), medtem ko je SCC zajemal SEM funkcionalnosti. Aprila 2009 so produkta združili in na trg ponudili SIEM rešitev z imenom **Enterprise Log Manager** (ELM). Od samega začetka produkt ne sodi v širši krog favoritov. Gartner ga je leta 2010 uvrstil v kvadrant izzivalcev, leta 2011 pa je celo izpadel iz magičnega kvadranta. Razlog, ki ga navaja Gartner [32], je v spremembi strategije podjetja CA. Obstoječi ELM produkt je CA preimenoval v User Activity Reporting Module in je sedaj del paketa za upravljanje identitet in dostopov (Identity and Access Management portfolio).

Ker smo pilota izvedli konec leta 2010, še nismo vedeli kakšna bo usoda produkta CA ELM. V nasprotnem primeru bi se zagotovo odločili za drugega ponudnika.

CA ponuja ELM le kot programski paket brez namenske naprave. To naj bi bila največja prednost pred ostalimi različicami. Poleg tega promovirajo enostavno nameščanje in nadgrajevanje agentov, visoko performančni zajem dogodkov, veliko kompresijo arhiviranih dnevnikov ter učinkovito analizo dogodkov. Učinkovita reklama se je v pilotski postavitvi izkazala za neresnično. Sledi vrednotenje različic.

6.4.4 Vrednotenje

Za nami so tri uspešne postavitve sistema SIEM v tesnem okolju. Želene cilje testiranja smo našteli v poglavju 6.3. Testiranja so potekala v razponu treh mesecev za vsako izmed različic. Ocenjevalno skupino so sestavljali trije bodoči skrbniki sistema SIEM. Razpon ocen je od 5 do 0 (5 – odlično, 4 – prav dobro, 3 – dobro, 2 – zadovoljivo, 1 – nezadovoljivo in 0 – različica ne vsebuje te funkcionalnosti). Sledi vrednotenje kriterijev za posamezno različico (končni rezultati so podani v tabeli 9).

Upravljanje dnevnikov in poročanje
To je najpomembnejši kriterij pri naši odločitvi, ki smo namenili dobro četrtino celotne ocene. ArcSight in enVision sta se odlično odrezala pri zajemu dnevnikov iz obstoječih varnostnih sistemov in nasploh celotne informacijske infrastrukture. To pa žal ne velja za CA-jev ELM. Pri slednjem smo naleteli na veliko težav pri zajemu dnevnikov (tako z agentom kot brez njega). Kar se tiče poročanja, ima enVision sistem že 1100 predpripravljenih poročil, ki jih je mogoče še dodatno prilagoditi lastnim potrebam. Vendar kljub temu da ima ArcSight manjše število predpripravljenih poročil, si zaslužil boljšo oceno, saj je njegov pristop izdelave pravil in korelacij daleč pred konkurenco. Odlikuje ga namreč izjemna enostavnost kreiranja poročil. Pri EML je izdelava poročil veliko težavnejše in zamudnejše opravilo.

Podpora za upravljanje incidentov
Test izdelave alarmiranja za deset kritičnih dogodkov je bil uspešen v vseh treh primerih, tako da je glavno vlogo pri oceni odigrala integracija z obstoječim orodjem SDM. Pri tem kriteriju je ELM dosegel najvišjo oceno (žal je tudi edina). Integracija ELM z obstoječim orodjem za upravljanje incidentov SDM je bila trivialna. To smo do neke mere tudi pričakovali, saj sta oba produkta plod CA razvijalcev. Tudi ostali dve različici nam je uspelo integrirati s SDM, ampak je bilo za dosego slednjega potrebno veliko več napora in dodatnega prilagajanja nastavitev znotraj SDM.

Namestitev in uporaba
ELM je bil v tem elementu daleč najslabši. Razlogov je več, med drugim problematična namestitev osnovne aplikacije, pogoste odpovedi glavnega servisa, počasno delovanje in celo okvara interne baze podatkov. Zaradi vseh teh problemov je ocenjevalna skupina začela dvomiti v primernost ELM rešitve. Kljub dvomom in negativnim občutkom nismo želeli izločiti ELM iz nadaljnjega testiranja. Pri ArcSight in enVision je bila osnovna namestitev opravljena v enem tednu (pri ELM je trajala cel mesec), tako da nam je posledično ostalo več časa za testiranja. Vsi proizvajalci ponujajo možnost izbire visoko razpoložljive konfiguracije. Pri tem je bila najbolj konkurenčna ponudba podjetja ArcSight. Končna postavitev je prikazana na sliki 20.

Spremljanje v realnem času
Izvedli smo nekaj tipskih napadov na IS, vendar smo pri merjenju ugotovili preveč različnih rezultatov. Primerjanje časov ne bi bilo pravično, saj je testiranje potekalo v različnih arhitekturnih postavitvah in na različno zmogljivih napravah. ELM je bil nameščen na bistveno manj zmogljiv strežnik, kot sta ga uporabljala ArcSight in enVision. Ocenjevalna skupina je določila vsem trem nevtralno oceno (3). Druga možnost bi bila, da bi ta kriterij izločili iz odločitvenega modela in ponovno preračunali uteži.

Korelacija dogodkov
Vzpostavili smo deset že predpripravljenih korelacij in dodali še pet lastnih. V tej kategoriji je nedvomni zmagovalec ArcSight. To se je nakazovalo že pri kreiranju poročil. Samo orodje za delo s korelacijami je izjemno intuitivno in ga je moč hitro usvojiti. Po enostavnosti in uporabnosti mu sledita enVision in ELM.

Spremljanje aplikacij
ArcSight in enVision podpirata obsežen seznam aplikacij. Zato zajem dnevnikov iz sporočilnega sistema Exchange, spletnega strežnika IIS in drugih aplikacij ni predstavljal problema. Medtem ko se je pri ELM zataknilo že pri IIS dnevnikih. Test je vseboval še zajem dnevnikov iz petih lastnih aplikacij (produkt internega razvoja aplikacij). Zadevo smo najlažje integrirali s sistemom ArcSight, saj se je izkazalo, da je uporaba format CEF najbolj enostavna od vseh različic.

Spremljanje podatkov
V testu smo izvedli samo povezavo na Oracle bazo. Zaradi pomanjkanja časa smo morali izpustiti testiranje zajema dogodkov za IBM DB2 in Microsoft SQL. Vse tri različice omogočajo nadzor sistema za upravljanje Oracle podatkovnih baz. S tem, da smo pri ELM (ponovno) naleteli na največ težav. Preveri smo tudi možnost uporabe DLP funkcionalnosti. RSA ponuja dodaten paket, t.i. RSA Data Loss Prevention Suite, ki ga je mogoče integrirati v RSA enVision. Slednjega nismo testirali, ker ni bil predviden kot del pilotske postavitve. Poleg tega enVision podpira še DLP rešitev podjetja Symantec in McAfee. ArcSight nima svoje DLP rešitve, temveč nudi podporo za rešitev podjetja Symantec in Fidelis. Podobno velja tudi za ELM, ki nudi le podporo lastnemu DLP produktu (CA Data Loss Prevention).

Spremljanje uporabnikov
Za osnovno spremljanje uporabniških aktivnosti je bilo najprej potrebno sistem SIEM integrirati z aktivnim imenikom. Tu ni bilo težav, saj je Microsoftov AD dobro podprt sistem. Nato smo kreirali osnovna poročila o uporabniških prijavah in odjavah v računalnik. Pri slednjem opravilu je ArcSight prejel najboljšo oceno. Navezave na ostale sisteme (HR, IdM) nismo izvedli, ker smo bili v času izbire sistema SIEM istočasno tudi v začetni fazi prenove HR sistema.

Nadzorna plošča
Ocenjevali smo prilagodljivost in preglednost nadzorne plošče. Največjo mero prilagodljivosti premore ArcSight rešitev. S pomočjo enostavnih nastavitev smo na osnovni strani prikazali trenutno zdravje IS oz. ključnih sistemov in določene kazalnike uspeha (število zaustavljenih napadov, število zaključenih incidentov idr.). Prilagodljivost in enostavnost ArcSight vmesnika je daleč pred konkurenco.

Končna ocena za določeno različico predstavlja vsota produktov uteži in ocene za določen kriterij. Na podlagi uteži w_i in ocen o_i za posamezen kriterij lahko izračunamo končno oceno različic po spodnji formuli, pri čemer je n število kriterijev ($n = 9$):

$$O = \sum_{i=1}^{n} w_i * o_i$$

	Uteži	ArcSight	RSA (EMC)	CA
upravljanje dnevnikov in poročanje	26%	5	4,5	3
podpora za upravljanje incidentov	16%	3,5	3,5	5
namestitev in uporaba	11%	4	4	1
spremljanje v realnem času	11%	3	3	3
korelacija dogodkov	11%	5	4	3
spremljanje aplikacij	11%	4,5	4	2,5
spremljanje podatkov	5%	4	5	2
spremljanje uporabnikov	5%	4	3	3
nadzorna plošča	5%	5	4	2
skupaj	**100%**	**4,33**	**3,98**	**2,98**

Tabela 10: Rezultati vrednotenja različic

Glede na zgornje rezultate vrednotenja različic je z oceno 4,33 zmagal ArcSight. Sledita mu RSA z oceno 3,98 in CA z najnižjo oceno 2,98. Vrstni red se ujema z dejansko uspešnostjo različic v testnem okolju. ArcSight se je izkazal pri vseh kriterijih in v polni meri izpolnil vsa pričakovanja in cilje, ki smo si jih zadali pred testno postavitvijo. Tudi integracijo z SDM smo uspeli obvladati in realizirati. RSA enVision je bil skozi celoten postopek testiranja resen tekmec ArcSight-u. Produkt enVision je zrel in profesionalen. Razlika med njima je le 0,35. Majhne razlike, ki so nastale med ArcSight in enVision gredo na račun ArcSight-ove enostavnejše analize dogodkov. Njegov pristop izdelave pravil in korelacij je daleč pred konkurenco. Na zadnjem mestu je različica CA ELM, kar ne preseneča. Težave so se vrstile skozi celoten postopek testiranja. Omenimo naj le nekatere:

- problematična osnovna namestitev aplikacije in agentov,
- počasno delovanje nadzornega spletnega vmesnika,
- pogoste odpovedi glavnega servisa,
- izguba interne baze podatkov,
- slaba ali nepopolna dokumentacija,
- slaba podpora s strani CA idr.

Kljub temu, da je bila različica ocenjena z oceno 3, je njena realna uporabnost veliko pod povprečjem in zato odsvetujemo njeno implementacijo. Poleg tega je aprila 2011 CA naznanil preoblikovanje produkta ELM v paket za upravljanje identitet in dostopov. Omenjeno je bil tudi glavni razlog, da ga je Gartner izključil iz magičnega kvadranta ponudnikov sistemov SIEM.

6.5 Realizacija odločitve

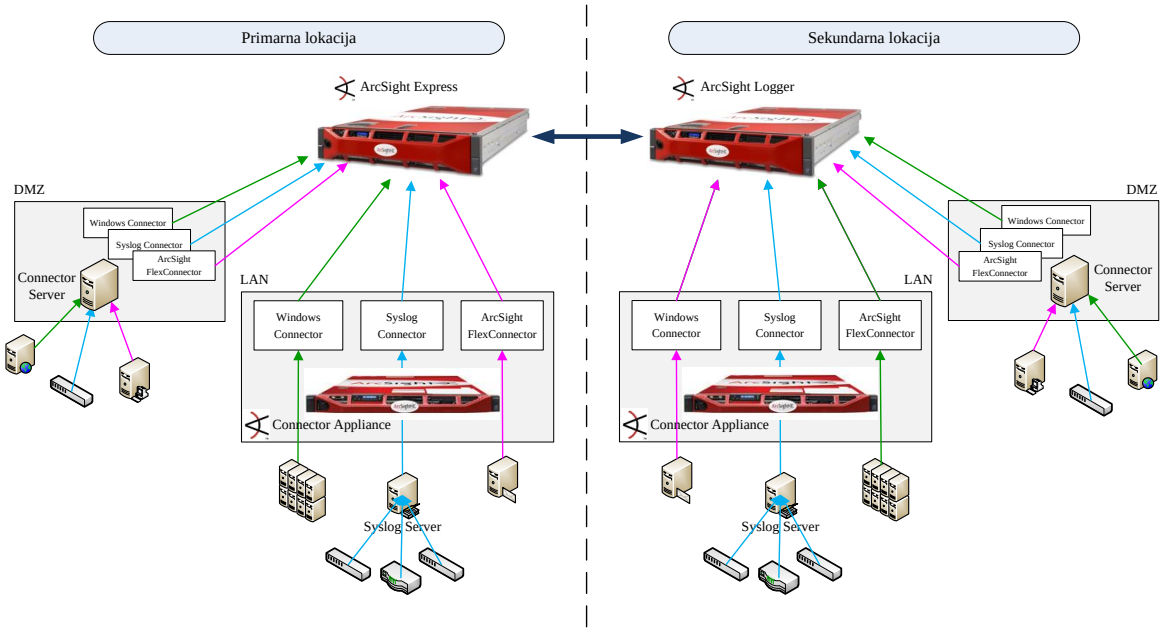
V prejšnji fazi smo na podlagi vrednotenja kriterij izbrali najboljšo različico ArcSight. Sedaj nastopi faza realizacije te odločitve. To pomeni, da začnemo dodeljevati sredstva za uresničitev različice in da je ta proces v splošnem nepovraten.

Končna postavitev ponudnika ArcSight se nekoliko razlikuje od testne postavitve (slika 18). Končna rešitev temelji na postavitvi visoko razpoložljive konfiguracije z zagotavljanjem geografske redundance in je sestavljena iz (slika 20):

- 1x ArcSight Express (M7200-X),
- 1x ArcSight Logger (L3200),
- 2x ArcSight Connector Appliance (C5200),
- 2x Connector server (obstoječi infrastrukturni strežnik).

Dodali smo en Connector Appliance in en Connector server. Connector Appliance je zmogljivejši kot v testu, saj zagotavlja še enkrat višji EPS (5000 EPS). S tem smo želeli nekoliko predimenzionirati celotni sistem. Celotna rešitev ArcSight SIEM zajemanja dnevnikov iz omrežne in strežniške infrastrukture je licencirana za zmožnost zajema do 2500 EPS in 750 naprav.

Na vsaki izbrani lokaciji (primarna in sekundarna) je en ArcSight Appliance, ki zajema dnevnike iz lokalnega omrežja in po en Connector Server za zajem dnevnikov iz DMZ. Za zajem nepodprtih dogodkov smo uporabili ArcSight FlexConnector, ki smo ga namestili na Connector Appliance in Connector Server. Glavna komponenta ArcSight Express je na primarni lokaciji. Razlog je v boljših performancah, ki se kažejo pri delu z nadzorno ploščo. Glede na to, da je večina uporabnikov sistema SIEM na primarni lokaciji, je bila odločitev trivialna. Na sekundarni lokaciji se nahaja ArcSight Logger. Ker se dogodki pošiljajo tako na Express kot Logger, je bilo nujno potrebno vzpostaviti izmenjavo podatkov med napravama. Slednja deluje na podlagi preprostega posredovanja dogodkov drugi napravi. Na ta način imata obe napravi vse potrebne informacije o dogajanju v IS.



Slika 20: ArcSight – končna postavitev

6.6 Gartnerjeva analiza

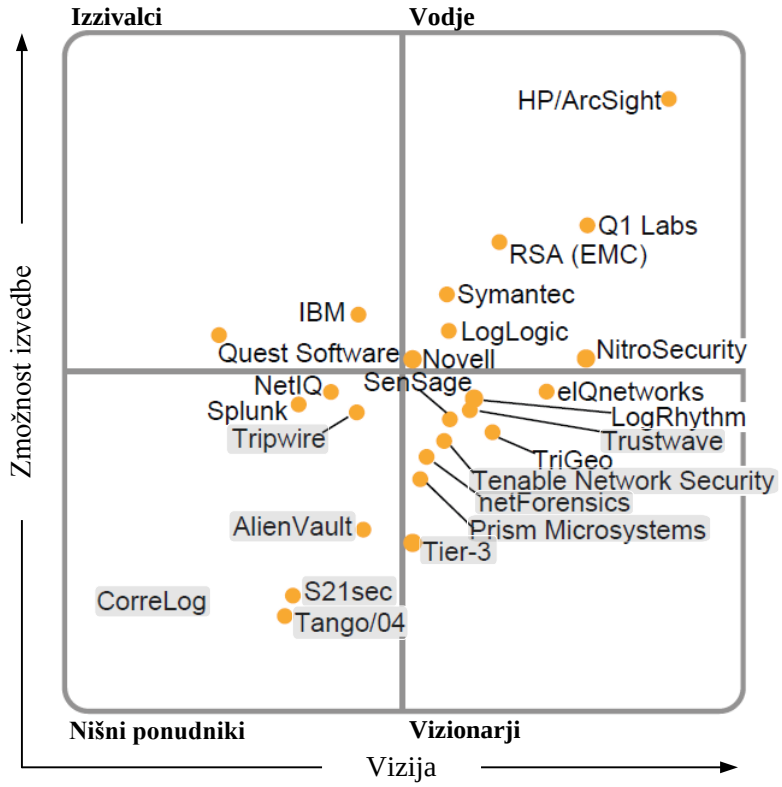
Analitska družba Gartner Group letno izdela nekaj manj kot sto analiz po metodologiji magičnega kvadranta. Magični kvadrant je raziskovalno orodje, ki ga je razvilo podjetje Gartner, ponuja pa rezultate in posnetke stanja na trgu v vizualni obliki. Preučuje usmerjenost podjetja, njegovo zrelost in zaposlene, ki ga oceni na podlagi izdelane vizije in realne zmožnosti za uresničitev vizije v praksi. Kvadrant ni namenjen komercialnim namenom, temveč predstavlja neodvisno znanstveno raziskavo tržnih dejstev.

V nadaljevanju sledi pregled Gartnerjeve analize SIEM produktov [32] in njegovih ključnih zmogljivost (angl. critical capabilities) [30].

Z analizo ključnih zmogljivosti želi Gartner olajšati delo pri začetni izbiri SIEM produkta. V raziskavo je zajetih petnajst ponudnikov sistema SIEM, torej deset manj kot jih je predstavil v magičnem kvadrantu ponudnikov SIEM za leto 2011 (slika 21). Razlog za zožen nabor ponudnikov je v neizpolnjevanju spodnjih kriterijev, ki jih je postavil Gartner:

- produkti morajo vsebovati vse glavne SIEM funkcionalnosti,
- produkti morajo biti v prodaji in v uporabi vsaj od januarja 2011 dalje,
- produkti morajo biti naravnani, da izpolnjujejo zahteve SIEM tržišča,
- ponudnik mora biti razpoznaven na svojem tržišču in imeti dovolj velik dohodek od prodaje.

Ponudniki, ki niso izpolnjevali navedenih kriterijev, so označeni s sivo barvo (AlienVault, CorreLog, netForensics, Prism Microsystems, S21sec, Tango/04, Tenable, Network Security, Tier-3, Tripwire in Trustwave). Iz kvadranta je razvidno, da gre predvsem za nišne ponudnike in izzivalce.



Slika 21: Gartnerjev magični kvadrant ponudnikov SIEM (maj 2011)

Analiza je zasnovana na ocenjevanju šestih ključnih zmogljivosti za tri najbolj pogoste tipe postavitve sistema SIEM:

a) zagotavljanje skladnosti,
b) obvladovanje groženj,
c) polna SIEM funkcionalnost.

Tudi Gartner je za svoj odločitveni problem uporabil metodo uteži parametrov (tabela 11).

Ključne zmogljivosti	**Zagotavljanje skladnosti**	**Obvladovanje groženj**	**SIEM**
upravljanje dnevnikov in poročanje	59.0%	10.0%	25.0%
upravljanje varnostnih dogodkov	2.0%	50.0%	35.0%
spremljanje podatkov	2.0%	15.0%	10.0%
spremljanje uporabnikov	5.0%	15.0%	10.0%
spremljanje aplikacij	2.0%	5.0%	10.0%
namestitev in podpora	30.0%	5.0%	10.0%
skupaj	100.0%	100.0%	100.0%

Tabela 11: Prikaz ključnih zmogljivosti in njihovih uteži za tri tipe postavitve

a) Zagotavljanje skladnosti

Postavitev sistema SIEM je v tem konkretnem primeru podrejena upravljanju dnevnikov in poročanju, zato ima tudi največjo utež. Na drugem mestu je namestitev in podpora. Od produkta pričakujemo, da bo čas postavitve čim krajši in njegova uporaba preprosta. Pri tem se upošteva tudi število predpripravljenih poročil za zagotavljanje skladnosti. Ostali kriteriji imajo zanemarljivo težo, razen spremljanja uporabnikov. Slednja funkcionalnost se uporablja pri spremljanju uporabniških dostopov do raznih virov znotraj IS. Zbrane informacije se uporabijo za namene poročanja.

b) Obvladovanje groženj

Če je primarni cilj postavitve sistema SIEM obvladovanje groženj, potem je toliko večja osredotočenost na upravljanje varnostnih dogodkov oz. SEM funkcionalnosti. Poudarek je na spremljanju dogajanja v realnem času, podpori za upravljanje incidentov ter izvajanju korelacij in analiz. S petnajstimi odstotki mu sledita spremljanje podatkov in uporabnikov, ki sta pomemben vir dodatnih informacij, ko gre za obravnavo internih groženj. SIM funkcionalnosti prav tako igrajo pomembno vlogo, saj se uporabljajo pri odkrivanju zunanjih groženj. Običajno je čas postavitve daljši kot v prvem primeru, zato tudi ni posebnega poudarka na tej zmogljivosti.

c) Polna SIEM funkcionalnost

V tem primeru želi podjetje izkoristiti vse kar mu lahko ponudi sistem SIEM. Podjetje želi zapolniti skladnostne vrzeli in uspešno obvladovati grožnje. Obe zmogljivosti skupaj predstavljata šestdeset odstotkov. Ostale štiri zmogljivosti so enakovredno utežene. Namestitev je v tem primeru najdaljša, predvsem na račun različnih sistemov, ki jih moramo med seboj povezati. Zato je pomembno, da se najprej vzpostavijo SIM funkcionalnosti in šele zatem vse ostale.

V tabeli 12 so prikazani rezultati vrednotenja produktov glede na kritične zmogljivosti.

	eIQnetworks	HP/ArcSight	IBM	LogLogic	LogRhythm	NetIQ	NitroSecurity	Novell	Q1 Labs	Quest Software	RSA (EMC)	SenSage	Splunk	Symantec	TriGeo
upravljanje dnevnikov in poročanje	3,5	4,1	2,8	4,0	3,6	3,0	3,7	3,2	4,0	2,9	3,5	4,0	3,0	3,4	3,2
upravljanje varnostnih dogodkov	3,4	4,7	2,0	3,0	2,8	1,6	3,5	4,2	4,2	2,0	3,2	2,5	1,8	3,7	3,0
spremljanje podatkov	3,3	3,1	2,8	3,1	3,2	2,9	4,0	2,6	3,2	1,0	3,4	3,0	1,6	2,7	3,2
spremljanje uporabnikov	3,4	4,3	4,0	2,6	3,0	3,0	3,4	4,0	3,7	3,1	3,3	3,5	1,0	2,2	3,2
spremljanje aplikacij	3,0	3,5	2,7	2,0	3,0	1,6	3,4	2,6	3,2	1,5	3,4	3,8	1,4	2,9	2,2
namestitev in podpora	3,2	3,0	2,6	3,6	4,2	2,8	3,5	2,6	3,5	3,0	3,2	2,8	2,5	3,5	4,5

Tabela 12: Ocena produktov glede na kritične zmogljivosti

Tabela 13 prikazuje ocene produktov za tri najbolj pogoste tipe postavitve sistema SIEM. Te informacije so odločevalcu v veliko pomoč, saj je mogoče v trenutku razbrati kateri produkti so zanimivi za nadaljnjo obravnavo (✔ in ❗) in kateri niso (✘).

	eIQnetworks	HP/ArcSight	IBM	LogLogic	LogRhythm	NetIQ	NitroSecurity	Novell	Q1 Labs	Quest Software	RSA (EMC)	SenSage	Splunk	Symantec	TriGeo
zagotavljanje skladnosti	3,4	3,8	2,8	3,7	3,7	2,9	3,6	3,1	3,8	2,9	3,4	3,6	2,7	3,4	3,6
obvladovanje groženj	3,4	4,2	2,6	3,0	3,0	2,2	3,6	3,7	3,9	2,1	3,3	3,0	1,8	3,2	3,1
polna SIEM funkcionalnost	3,4	4,1	2,6	3,2	3,2	2,3	3,6	3,5	3,8	2,3	3,3	3,2	2,0	3,3	3,2
skupna ocena	❗	✔	✘	❗	❗	✘	✔	❗	✔	✘	❗	❗	✘	❗	❗

Tabela 13: Ocena produktov glede na tip postavitve

7. Sklepne ugotovitve

Glavna motivatorja za postavitev sistema za upravljanja varnostnih informacij in dogodkov v banki sta bila centralizirano upravljanje dnevnikov in izboljšati proces upravljanja incidentov. Projekta smo se lotili z analizo stanja, ki je pokazala, da bi z vzpostavitvijo sistema SIEM zadovoljili obema ciljema. Sledila je začetna izbira SIEM ponudnikov s katerimi smo opravili trimesečno testiranje v našem IS. Po končanem testiranju smo s pomočjo postavljenega odločitvenega modela izbrali najustreznejšo različico (ArcSight).

Vzpostavitev sistema SIEM je kompleksen projekt, saj je sistem potrebno povezati s celotnim IS. Od članov projekta se pričakuje dobro poznavanje obstoječe informacijske infrastrukture in predanost projektu. Poleg usposobljenega kadra je potrebno zagotoviti sredstva za nakup sistema SIEM. Ponudbe za vzpostavitev takega sistema, kot smo ga predstavili v končni postavitvi (slika 20) se gibljejo med 150.000 in 200.000 evri. Obstajajo tudi odprtokodne rešitve (Splunk, OSSIM, Sguil, Microsoft Log Parser idr.), katere so primerne le za majhna okolja oz. za domačo rabo. Večina teh orodij ne vsebuje vseh SIEM funkcionalnosti in zato niso primerna za večja okolja. Vsekakor pa se je dobro zavedati, da taka orodja obstajajo in da jih lahko vključimo v proces odločanja. Naslednji problem, ki se je pojavil je dolžina trajanja projekta. Najhitrejše so postavitve tipa "zagotavljanje skladnosti", ki od arhitekta zahtevajo le vključitev vseh naprav v sistem SIEM. Če še predpostavimo, da gre za enostavno arhitekturno rešitve, potem je čas trajanja vzpostavitve od tri do šest mesecev. Najdaljši so projekti kjer se odločimo za vzpostavitev sistema s polno SIEM funkcionalnostjo. Pri slednjih lahko proces postavitve traja tudi do več let. V našem primeru projekt po letu in pol še vedno ni zaključen. Glavna razloga za to sta kompleksnost rešitve in pomanjkanje časa oz. kadra. Če želimo kvalitetno izkoristili sistem SIEM, se je potrebno z njim tudi ukvarjati. Sistem SIEM ni rešitev za vse naše težave, temveč je le orodje s katerim si olajšamo delo. Priporoča se, da je SIEM skrbnik polno zaposlen samo s sistemom SIEM.

Dodana vrednost magistrskega dela je v ponovljivosti postopka. Ne glede na izbrane ponudnike, lahko odločevalec izbere poljubne SIEM ponudnike in uporabi opisano metodologijo. Odločevalcu je v pomoč seznam kriterijev za vrednotenje različic sistema SIEM, ki smo ga predstavili v tabeli 9. Odločevalec se mora opredeli za eno izmed treh najbolj pogostih tipov postavitve (zagotavljanje skladnosti , obvladovanje groženj in polna SIEM funkcionalnost) ter določiti uteži za posamezni kriterij. Pri tem si lahko pomaga s predstavljeno študijo ali z Gartnerjevo analizo.

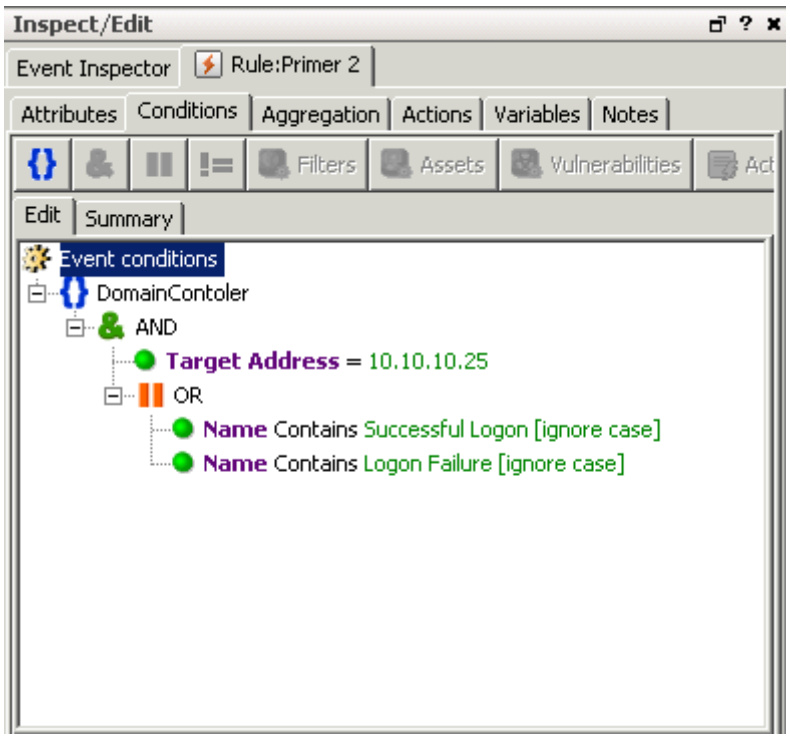
PRILOGA – Praktični del

Na sliki 22 je prikazan zajem dogodkov v dvominutnem intervalu. Dogodki so razvrščeni po prioriteti oz. pomembnosti (stolpec "Priority"). Zaradi zaupnih podatkov sta izvorni IP (stolpec "Attacker Address") in ponorni IP (stolpec "Target Address") namenoma neberljiva.

End Time	Name	Attacker Address	Target Address	Priority	Device Vendor	Device Product
9 avg 2011 10:01:51 CEST	HTTP_IIS_Unicode_Wide_Encoding			9	ISS	Proventia G-Series
9 avg 2011 10:01:51 CEST	Attack from Source having Reconnaissance History			9	ArcSight	ArcSight
9 avg 2011 10:01:51 CEST	Attack From Suspicious Source			9	ArcSight	ArcSight
9 avg 2011 10:01:51 CEST	Compromise - Attempt			9	ArcSight	ArcSight
9 avg 2011 10:00:09 CEST	Suspicious Communication From Attacked Target			9	ArcSight	ArcSight
9 avg 2011 10:02:06 CEST	HTTP_IIS_Unicode_Wide_Encoding			8	ISS	Proventia G-Series
9 avg 2011 10:01:44 CEST	Logon Failure			8	Microsoft	Microsoft Windows
9 avg 2011 10:01:44 CEST	Logon Failure			8	Microsoft	Microsoft Windows
9 avg 2011 10:01:44 CEST	Logon Failure			8	Microsoft	Microsoft Windows
9 avg 2011 10:01:41 CEST	Device connection down			8	ArcSight	ArcSight
9 avg 2011 10:01:33 CEST	Logon Failure			8	Microsoft	Microsoft Windows
9 avg 2011 10:01:33 CEST	Logon Failure			8	Microsoft	Microsoft Windows
9 avg 2011 10:01:33 CEST	Logon Failure			8	Microsoft	Microsoft Windows
9 avg 2011 10:02:06 CEST	IIS action			7	Microsoft	Internet Information Server
9 avg 2011 10:02:06 CEST	IIS action			7	Microsoft	Internet Information Server
9 avg 2011 10:02:06 CEST	IIS action			7	Microsoft	Internet Information Server
9 avg 2011 10:02:05 CEST	IIS action			7	Microsoft	Internet Information Server
9 avg 2011 10:02:05 CEST	IIS action			7	Microsoft	Internet Information Server
9 avg 2011 10:01:59 CEST	HTTP_Put			7	ISS	Proventia G-Series
9 avg 2011 10:00:00 CEST	Successful Configuration Change			7	ArcSight	ArcSight
9 avg 2011 10:00:23 CEST	HTTP_URL_repeated_char			6	ISS	Proventia G-Series
9 avg 2011 10:00:15 CEST	HTTP_IIS_UTF8_Evasion			6	ISS	Proventia G-Series
9 avg 2011 10:02:06 CEST	Fan service recommended			5	CISCO	CiscoRouter
9 avg 2011 10:01:57 CEST	The Windows Filtering Platform blocked a packet.			5	Microsoft	Microsoft Windows
9 avg 2011 10:01:55 CEST	Drop Rate Exceeded			5	CISCO	ASA
9 avg 2011 10:01:45 CEST	Drop Rate Exceeded			5	CISCO	ASA
9 avg 2011 10:01:44 CEST	The Windows Filtering Platform blocked a packet.			5	Microsoft	Microsoft Windows
9 avg 2011 10:01:44 CEST	The Windows Filtering Platform blocked a packet.			5	Microsoft	Microsoft Windows
9 avg 2011 10:01:42 CEST	The Windows Filtering Platform blocked a packet.			5	Microsoft	Microsoft Windows
9 avg 2011 10:00:10 CEST	Threshold exceeded for Blocked Category			5	Websense	Websense Enterprise and Policy Server
9 avg 2011 10:00:09 CEST	The Windows Filtering Platform blocked a packet.			5	Microsoft	Microsoft Windows
9 avg 2011 10:00:07 CEST	VBRuntime			5	Microsoft	System or Application Event
9 avg 2011 10:00:00 CEST	A privileged service was called.			5	Microsoft	Microsoft Windows
9 avg 2011 10:02:10 CEST	Successful Network Logon			4	Microsoft	Microsoft Windows
9 avg 2011 10:02:10 CEST	An account was successfully logged on.			4	Microsoft	Microsoft Windows
9 avg 2011 10:02:10 CEST	An account was successfully logged on.			4	Microsoft	Microsoft Windows
9 avg 2011 10:02:10 CEST	An account was successfully logged on.			4	Microsoft	Microsoft Windows
9 avg 2011 10:02:10 CEST	The Windows Filtering Platform has allowed a co...			4	Microsoft	Microsoft Windows
9 avg 2011 10:02:10 CEST	An account was logged off.			4	Microsoft	Microsoft Windows
9 avg 2011 10:02:10 CEST	An account was successfully logged on.			4	Microsoft	Microsoft Windows
9 avg 2011 10:02:10 CEST	An account was logged off.			4	Microsoft	Microsoft Windows
9 avg 2011 10:01:57 CEST	Received SNMP packet(s) from UDP: [127.0.0.1...			4	Unix	Unix
9 avg 2011 10:01:57 CEST	Connection from UDP: [127.0.0.1]:59699			4	Unix	Unix
9 avg 2011 10:01:57 CEST	Received SNMP packet(s) from UDP: [127.0.0.1...			4	Unix	Unix
9 avg 2011 10:01:57 CEST	Connection from UDP: [127.0.0.1]:50680			4	Unix	Unix
9 avg 2011 10:02:07 CEST	Monitor Event			3	ArcSight	ArcSight
9 avg 2011 10:02:07 CEST	RECEIVE			3	Microsoft	Exchange Server
9 avg 2011 10:02:07 CEST	Oracle.grid			3	Microsoft	System or Application Event
9 avg 2011 10:02:07 CEST	Oracle.grid			3	Microsoft	System or Application Event
9 avg 2011 10:00:57 CEST	VMware ESX VMware[init] events			2	VMware	ESX
9 avg 2011 10:00:57 CEST	VMware ESX VMware[init] events			2	VMware	ESX
9 avg 2011 10:00:57 CEST	VMware ESX VMware[init] events			2	VMware	ESX

Slika 22: Pregled dogodkov v ArcSight konzoli

V poglavju 4.2 smo med drugim predstavili tudi izdelavo pravil. Na sliki 23 je prikazana izdelava pravila znotraj ArcSight konzole za primer 2 (stran 31), ki prikaži vse domenske prijave na domenski strežnik s ponornim naslovom 10.10.10.25.



Slika 23: Izdelava pravila

Seznam slik

Slika 1: CIA trojček 6
Slika 2: Demingov krog 7
Slika 3: Piramida dokumentov, ki definirajo SUVI v organizaciji 8
Slika 4: Pregled standardov ISO/IEC 27000 9
Slika 5: Struktura standarda ISO/IEC 27001:2005 10
Slika 6: ITIL v3 življenjski krog storitev 12
Slika 7: Primer procesa upravljanja dogodkov 15
Slika 8: Primer procesa upravljanja incidentov 18
Slika 9: Relacije med izrazi 23
Slika 10: SIEM arhitektura 29
Slika 11: Diagram poteka – oddaljene prijave lokalnih administratorjev 32
Slika 12: Časovni prikaz dogodkov v primeru alarma 33
Slika 13: Faze odločitvenega procesa 53
Slika 14: Zrelost procesa upravljanja dogodkov 56
Slika 15: Zrelost procesa upravljanja incidentov 57
Slika 16: Gartnerjev magični kvadrant ponudnikov SIEM (maj 2010) 58
Slika 17: ArcSight arhitekturne komponente 62
Slika 18: ArcSight – testna postavitev 65
Slika 19: RSA – primer LS arhitekture 67
Slika 20: ArcSight – končna postavitev 71
Slika 21: Gartnerjev magični kvadrant ponudnikov SIEM (maj 2011) 72
Slika 22: Pregled dogodkov v ArcSight konzoli 76
Slika 23: Izdelava pravila 77

Seznam tabel

Tabela 1: Primer zajema dogodkov v dvajset sekundnem intervalu 31
Tabela 2: Predpisan čas hranjenja dnevnikov za določen standard 34
Tabela 3: Pregled standardov SCAP in njihov namen 39
Tabela 4: Statistični podatki o uporabi OS 47
Tabela 5: Prikaz SWOT matrike 54
Tabela 6: SWOT analiza za uvedbo sistema SIEM 55
Tabela 7: Izbrani ponudniki za testno postavitev 58
Tabela 8: Določitev kriterijev in uteži za vrednotenje različic sistema SIEM 60
Tabela 9: Seznam kriterijev za vrednotenje različic sistema SIEM 61
Tabela 10: Rezultati vrednotenja različic 70
Tabela 11: Prikaz ključnih zmogljivosti in njihovih uteži za tri tipe postavitve 73
Tabela 12: Ocena produktov glede na kritične zmogljivosti 74
Tabela 13: Ocena produktov glede na tip postavitve 74

Viri

[1] S. Adams, A. Cartlidge, A. Hanna, J. A. Sowerby, J. Windenbank, *ITIL V3 Foundation Handbook*, Norwich, U.K: The Stationery Office, 2008.

[2] M. Bohanec, *Odločanje in modeli*, Ljubljana: DMFA - založništvo, 2006.

[3] A. Brezavšček, S. Moškon, "Vzpostavitev sistema za upravljanje informacijske varnosti v organizaciji," *Uporabna informatika*, letnik 18, št. 2, str. 101-108, 2010.

[4] A. Chuvakin (2007), Six Mistakes of Log Management. Dostopno na: http://www.infosecwriters.com/text_resources/pdf/Six_Mistakes_of_Log_Management_AChuvakin.pdf

[5] B. T. Contos, C. Derodeff, W. P. Crowell, D. Dunkel, *Physical and Logical Security Convergence*, Burlington, MA: Syngress Publishing, Inc., 2007, pogl. 5.

[6] S. Diver (2007) Information Security Policy – A Development Guide for Large and Small Companies. Dostopno na: http://www.sans.org/reading_room/whitepapers/policyissues/information-security-policy-development-guide-large-small-companies_1331

[7] M. Howard, D. LeBlanc, J. Viega, *24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them*, New York: McGraw-Hill, 2009.

[8] M. Krisper, COBIT, prosojnice s predavanj pri predmetu Teorija informacijskih sistemov, podiplomski študij Računalništva in informatike, Fakulteta za računalništvo in informatiko, Univerza v Ljubljani, 2006.

[9] H. Marquis (2006), A prescription for ITIL. Dostopno na: http://www.itsmsolutions.com/newsletters/DITYvol2iss11.htm

[10] M. Marušič, *SWOT analiza podjetja PU-MA d.o.o.*, diplomsko delo. Ljubljana: Ekonomska fakulteta, 2005.

[11] D. R. Miller, S. Harris, A. A. Harper, S. VanDyke, C. Blask, *Security Information and Event Management (SIEM) Implementation*, New York: McGraw-Hill, 2010, pogl. 5.

[12] C. Perrin (2008), The CIA Triad. Dostopno na: http://www.techrepublic.com/blog/security/the-cia-triad/488

[13] M. V. Ramana Murthy, P. Ram Kumar, E. Devender Rao, A C Sharma, S. Rajender, S. Rambabu, "Performance of the Network Intrusion Detection Systems," *International Journal of Computer Science and Network Security*, št. 9, zv.10, str. 198-202, 2009.

[14] S. Taylor, D. Cannon, D. Wheeldon, *ITIL Version 3 Service Operation*, London, U.K: The Stationery Office, 2007.

[15] T. Vidmar, *Informacijsko-komunikacijski sistem*, Ljubljana: Pasadena, 2002.

[16] P. Zabukovec, *Vzpostavitev službe za podporo uporabnikom*, diplomsko delo. Maribor: Fakulteta za organizacijske vede, 2008.

[17] L. Zupan, A. Brezavšček, "Novosti, ki jih prinašajo spremembe standarda BS 7799," *Organizacija*, letnik 39, št. 1, str. 58-66, 2006.

[18] (2004) Uradni list RS, št. 83/2004 z dne 29.7.2004. Dostopno na: http://www.uradni-list.si/1/objava.jsp?urlid=200483&stevilka=3735

[19] (2005) ISO/IEC 27001:2005. Dostopno na: http://www.cert.sd/iso27001.pdf

[20] (2005) ISO/IEC 27002:2005. Dostopno na: http://www.cert.sd/iso27002.pdf

[21] (2006) Guide to Computer Security Log Management, NIST SP800-92. Dostopno na: http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf

[22] (2007) Incident Management - Incident prioritization. Dostopno na: http://www.itilfoundations.com/processes/incident-management/priority/

[23] (2007) Načini varovanja ter zdravljenja podatkov. Dostopno na http://colos1.fri.uni-lj.si/ERI/INFORMATIKA/RACUNALNISKA_OMREZJA/NaciniVarovanjaZdravljenjaPodatkov.html
[24] (2007) The Intrusion Detection Message Exchange Format (IDMEF). Dostopno na: http://tools.ietf.org/html/rfc4765
[25] (2009) Cisco MARS shuts out new third-party security devices. Dostopno na: http://www.networkworld.com/news/2009/110609-cisco-mars.html
[26] (2009) SANS - Effective Use Case Modeling for SIEM. Dostopno na: http://www.sans.org/reading_room/whitepapers/auditing/effective-case-modeling-security-information-event-management_33319
[27] (2010) Magic Quadrant for Security Information and Event Management. Dostopno na: http://www.arcsight.com/collateral/whitepapers/Gartner_Magic_Quadrant_2010.pdf
[28] (2010) Monitoring up the Stack: Adding Value to SIEM. Dostopno na: http://securosis.com/reports/Securosis-Monitoring_up_the_Stack_FINAL.pdf
[29] (2011) ArcSight - Supported Products. Dostopno na: http://www.arcsight.com/collateral/ArcSight_Supported_Products.pdf
[30] (2011) Critical Capabilities for Security Information and Event Management Technology. Dostopno na: http://www.arcsight.com/library/download/Gartner-SIEM-Critical-Capabilities-for-SIEM-2011/
[31] (2011) Inside Gartner Research. Dostopno na: http://imagesrv.gartner.com/research/methodologies/inside_gartner_research.pdf
[32] (2011) Magic Quadrant for Security Information and Event Management. Dostopno na: http://www.arcsight.com/collateral/whitepapers/Gartner_Magic_Quadrant_2011.pdf
[33] (2011) OS Platform Statistics. Dostopno na: http://www.w3schools.com/browsers/browsers_os.asp
[34] (2011) SANS Seventh Annual Log Management Survey Report. Dostopno na: http://www.arcsight.com/collateral/whitepapers/ArcSight_SANS_2011_Log_Management_Survey.pdf
[35] (2011) The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.1, NIST SP800-126. Dostopno na: http://csrc.nist.gov/publications/nistpubs/800-126-rev1/SP800-126r1.pdf