KAUNO TECHNOLOGIJOS UNIVERSITETAS

INFORMATIKOS FAKULTETAS

Povilas Ivanovas

Incidentų kompiuterių tinkluose identifikavimas, taikant anomalijų aptikimo metodus

Baigiamasis magistro darbas

Vadovas
Prof. Algimantas Venčkauskas

KAUNAS, 2017

KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ KATEDRA

TVIRTINU
Katedros vedėjas
(parašas) Prof. Algimantas Venčkauskas
(data)

Incidentų kompiuterių tinkluose identifikavimas, taikant anomalijų aptikimo metodus

Baigiamasis magistro darbas

Informacijos ir informacinių technologijų sauga (kodas 621E10003)

Vadovas
(parašas) Prof. Algimantas Venčkauskas
(data)

Recenzentas
(parašas) Doc. dr. Rimantas Kavaliūnas
(data)

Projektą atliko
(parašas) Povilas Ivanovas
(data)

KAUNAS, 2017

KAUNO TECHNOLOGIJOS UNIVERSITETAS

Informatikos

(Fakultetas)

Povilas Ivanovas

(Studento vardas, pavardė)

Informacijos ir informacinių technologijų sauga (kodas 621E10003)

(Studijų programos pavadinimas, kodas)

„Baigiamojo projekto pavadinimas“

AKADEMINIO SĄŽININGUMO DEKLARACIJA

20 17 m. birželio 2 d.

Kaunas

Patvirtinu, kad mano **Povilo Ivanovo** baigiamasis projektas tema „Incidentų kompiuterių tinkluose identifikavimas, taikant anomalijų aptikimo metodus“ yra parašytas visiškai savarankiškai, o visi pateikti duomenys ar tyrimų rezultatai yra teisingi ir gauti sąžiningai. Šiame darbe nei viena dalis nėra plagijuota nuo jokių spausdintinių ar internetinių šaltinių, visos kitų šaltinių tiesioginės ir netiesioginės citatos nurodytos literatūros nuorodose. Įstatymų nenumatytų piniginių sumų už šį darbą niekam nesu mokėjęs.

Aš suprantu, kad išaiškėjus nesąžiningumo faktui, man bus taikomos nuobaudos, remiantis Kauno technologijos universitete galiojančia tvarka.

(vardą ir pavardę įrašyti ranka) *(parašas)*

Ivanovas, P. „Incidentų kompiuterių tinkluose identifikavimas, taikant anomalijų aptikimo metodus“. Magistro baigiamasis projektas / vadovas Prof. Algimantas Venčkauskas; Kauno technologijos universitetas, informatikos fakultetas, kompiuterių katedra.

Kaunas, 2017. 58 p.

SANTRAUKA

„Incidentų kompiuterių tinkluose identifikavimas, taikant anomalijų aptikimo metodus“ – tai identifikavimo metodai, kurie teikia administratoriui informaciją apie tinkle vykstančias anomalijas ir incidentus. Šių metodų pagalba siekiama laiku pastebėti, identifikuoti, reaguoti į anomalijas ir incidentus, kol nepadaryta didesnė žala. Analizės dalyje pateikta dažniausiai sutinkamų kompiuteriniuose tinkluose incidentų klasifikacija. Taip pat pateikti tinklo anomalijų aptikimo metodai. Renkantis saugos informacijos įvykių valdymo ir saugojimo sistemą atlikta panašių sistemų analizė. Daroma išvada, jog pasirinkta saugos informacijos įvykių valdymo ir saugojimo sistema atitinka visus iškeltus reikalavimus. Kitoje dalyje aprašomas pasirinktos saugos informacijos įvykių valdymo ir saugojimo sistemos projektavimas. Aprašius sistemos aktorius (administratorius, sistema) ir jų panaudos atvejus, pateikti funkciniai ir nefunkciniai sistemos reikalavimai. Pagal šiuos reikalavimus, realizuojama pasirinkta sistema. Po projektinės dalies atliekama realizacija bei gaunami tyrimo rezultatai. Išvadose pateikiamas viso darbo apibendrinimas.

Ivanovas, Povilas. *Incident Identification of Computer Networks Using Anomaly Detection Methods*. Master thesis / research supervisor Assoc. Prof. Algimantas Venčkauskas. The Faculty of Informatics, Kaunas University of Technology.

Kaunas, 2017. 58 p.

SUMMARY

"Incident Identification of computer networks using anomaly detection methods" – it is identification methods that provide information about anomalies and incidents in the administrated networks. These methods help to timely notice, identify, react to anomalies and incidents while it has not made more damage. The analytical part of the most commonly occurring incidents classification of computer networks and network anomaly detection methods are presented. When choosing a security information and event management system analysis of similar systems was made. The conclusion is that the choice of security information event management and storage system conforms to all requirements. The next part describes the selected security information event management and storage system project. After defining the actors (administrator, system) and their use cases there are distinguished functional and non-functional system requirements in accordance with the requirements system was realized. After the design of the system follows the realization and received results. In the summary conclusions of the work a presented.

TURINYS

LENTELIŲ SĄRAŠAS

PAVEIKSLŲ SĄRAŠAS

TERMINŲ IR SANTRUMPŲ ŽODYNAS

Anomalija – nuokrypis nuo normos

DDoS – paskirstytas paslaugų blokavimas

DoS – Paslaugų blokavimas

IDS – įsibrovimo aptikimo sistema

IKT – informacijos ir komunikacijų technologijos

Incidentas – fiksuotas rezultatas, pagal iš anksto žinomus saugos pažeidžiamumų atakų modelius

NIDS – tinklo įsibrovimo aptikimo sistema

OSSEC – Atviro kodo apsauga

OSSIM – Atviro kodo informacijos saugumo ir įvykių valdymo sistema

SIEM – Informacijos saugumo ir įvykių valdymo sistema

Spam – nepageidaujami elektroninio pašto laiškai

USM – vieningas saugumo valdymas

ĮVADAS

Darbo problematika ir aktualumas. Šiomis dienomis kompiuteris ir internetas yra praktiškai neatsiejami gyvenimo įrankiai. Kompiuteris naudojamas tiek namuose laisvalaikiui praleisti, tiek darbui. Kompiuteriu mes galime apsipirkti internete, užsisakyti maisto į namus, pervesti pinigus kitam asmeniui, pasitikrinti banko sąskaitos likutį, apmokėti sąskaitas už komunalinius mokesčius, skaityti naujienas, susirašinėti su draugais, giminėmis ir dar daug viso kito. Retas atvejis, jog pas žmogų šiais laikais nerastum jokio kompiuterinio prietaiso, įskaitant mobiliuosius telefonus, planšetinius kompiuterius ir kt. kompiuterinius įrenginius.

Nors visa tai ir palengvina mūsų kasdieninį gyvenimą, bet už viso to slypi ir pavojai: yra tikimybė prarasti savo turimus pinigus iš banko sąskaitų, gali nutekėti jūsų konfidenciali / asmeninė informacija tretiems asmenims, gali būti sutrikdytas jūsų kasdieninis naudojimasis asmeniniu kompiuteriu, verslo veikla, sukompromituota / sutrikdyta internetinių paslaugų veikla.

Incidentai kompiuteriniuose tinkluose gali būti įvairūs: įžeidžiantis turinys – tai, nepageidaujami elektroninio pašto laiškai; kenksmingas kodas; informacijos rinkimas; bandymai įsibrauti. Anomalija – tai, nuokrypis nuo normos, nepageidaujama veikla mūsų teikiamoje ar saugojamoje paslaugoje.

Kompiuterinės įrangos naudotojai pirmiausia privalo pasirūpinti savo pačių saugumu ir užkirsti bet kokį kelią iki jų pačių ir neleisti programišiui pakenkti. Arba pirkti apsaugos priemones iš įmonių.

Šis magistrinis darbas sukoncentruotas į tam tikrus / pasirinktus incidentus ir nuokrypius nuo normos kompiuteriniuose tinkluose, svarbu laiku pastebėti, išanalizuoti ir reaguoti į incidentą ar nuokrypį nuo normos iki kol žalinga / kenksminga / kenkėjiška veikla nepadarė didesnės žalos mūsų sistemoje.

Darbo tikslas ir uždaviniai. Šios kuriamos sistemos tikslas: realiu laiku, automatiniu būdu aptikti anomalijas ir incidentus, realizacija atliekama OSSIM (angl. *Open Source Security Information and Event Management*) aplinkoje. Šios sistemos pagalba, tinklo administratorius gali lengviau identifikuoti ir reaguoti į incidentus.

Pagrindiniai šio darbo uždaviniai yra:

- sukurti OSSIM pagrindu sistemą renkančią įvykius iš įvairių šaltinių ir juos normalizuoti;
- sukurti ir realizuoti automatinio anomalijų (nuokrypis nuo normos) ir incidentų (fiksuotas rezultatas, pagal iš anksto žinomus saugos pažeidžiamumų atakų modelius) aptikimo algoritmus pasinaudojant OSSIM ir OSSEC esamomis priemonėmis;
- esamas incidentų ir įvykių sukūrimo taisykles papildyti naujomis, sukuriant panaudojant gaunamus įvykius unikalius metodus pritaikytus specifinei aplinkai.

Darbo struktūra. Šį magistrinį darbą sudaro šešios dalys. Pirmoji dalis yra įvadas, kurioje apžvelgiama problematika ir aktualumas, darbo tikslai ir struktūra. Antroje dalyje pateikiama analitinė dalis, kurioje analizuojami incidentai kompiuteriniuose tinkluose, anomalijų aptikimo metodai,

įsibrovimo aptikimo sistemos bei valdymo įrankiai. Trečioji yra projektinė dalis, kurioje pateikiama sistemos struktūra, funkciniai, nefunkciniai reikalavimai. Ketvirtoje dalyje pateikiama tyrimas. Penkta dalis yra rezultatų apibendrinimas ir išvados. Šeštoje dalyje pateikta naudota literatūra.

1. INCIDENTŲ KOMPIUTERIŲ TINKLUOSE IDENTIFIKAVIMAS, TAIKANT ANOMALIJŲ APTIKIMO METODUS ANALITINĖ DALIS

1.1. Incidentai kompiuteriniuose tinkluose

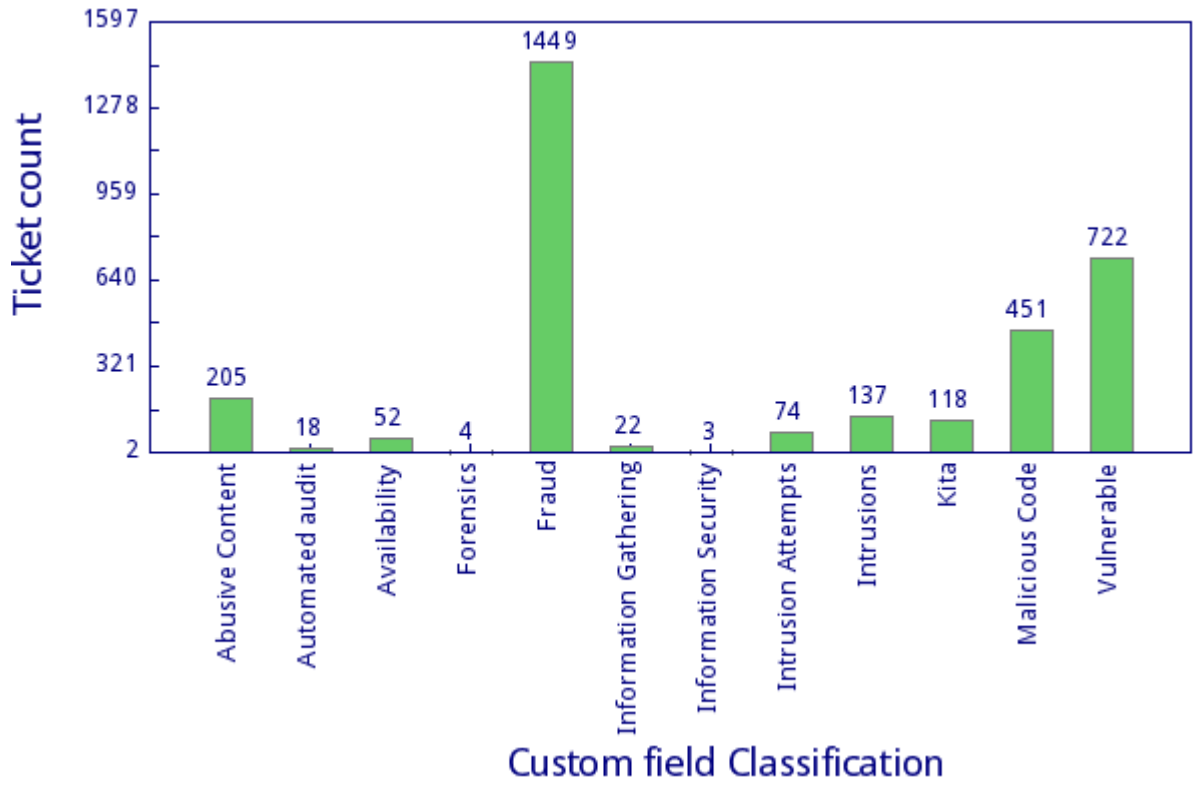
Šiame skyriuje pateikiami incidentų klasifikacija, kurie dažniausiai sutinkami internetinėje erdvėje [1]:

1) įžeidžiantis turinys – dažniausiai toks turinys atkeliauja į elektroninio pašto dėžutę su įvairiausiu turiniu:
   - elektroninio pašto laiškai (angl. *Spam*), gaunami kaip reklama;
   - klaidinanti, kompromituojanti informacija apie jus, jūsų šeimą, giminaičius ar draugus;
   - apgaulingas laiškas su nuoroda į svetainę, kurioje prašoma įvesti savo asmeninę informaciją, banko sąskaitų informaciją ir kt.;
   - apgaulingas laiškas su žalingą kodą turinčiu priedu, prikabintu prie laiško, atidarius minėtą failą, užkrečiamas kompiuteris;
2) žalingas / kenksmingas kodas yra orientuotas į operacines sistemas, labiausiai paplitęs „Microsoft Windows“ operacinėse sistemose, taip pat daugėja atvejų, jog mobilieji telefonai apsikrečia kenksmingu kodu. Žalingas kodas turi ne vieną paskirtį:
   - trinti, šifruoti bylas;
   - atlikti kenkėjišką veiklą iš užkrėsto kompiuterio;
   - rinkti informaciją apie jus, jūsų naršymo istoriją, asmeninį gyvenimą;
3) informacijos rinkimas – tai ataka, kai siunčiamos užklausos į sistemą ir ieškomos silpnos vietos ar stebimas ir įrašomas tinklo srautas;
4) bandymai įsibrauti vyksta sukompromituojant sistemą arba sutrikdant tos sistemos bet kokią paslaugą, išnaudojant silpnąsias vietas, pvz. duomenų perpildymo klaida (angl. *buffer overflow*), galinės / užpakalinės durys (angl. *backdoor*). Taip pat bandymai atspėti vartotojo slaptažodį įvairiais būdais: spėjant, naudojant scenarijų ir kt.;
5) prieinamumas – *DoS, DdoS* siunčiamas didelis kiekis paketų į atakuojamą tašką. Šiuo būdu sutrikdoma įprastinė atakuojamos paslaugos veikla. Bei dažnai šios atakos metu išryškėja silpnosios atakuojamos internetinės paslaugos vietos;
6) sukčiavimas – tai nelegaliu būdu įsigyti filmai, muzika, žaidimai, programinė įranga.

Šioje 1.1 lentelėje pateikiama incidentų klasifikacija [1]:

1.1 lentelė Incidentų klasifikacija

Incidento klasė	Incidento tipas
Įžeidžiantis turinys	Nepageidaujami elektroninio pašto laiškai (angl. *Spam*)
	Priekabiavimas
	Vaikai / seksualinis / smurtas /...
Kenksmingas kodas	Virusas
	Kirminas (angl. *worm*)
	Trojanas (angl. *trojan*)
	Šnipinėjimas
	Rinkiklis
Informacijos rinkimas	Skenavimas
	Šniukštinėjimas (angl. *Sniffing*)
	Socialinė inžinerija
Bandymai įsibrauti	Išnaudojama žinomais pažeidžiamumais
	Prisijungimų bandymai
	Naujos nežinomos atakos bandant patekti į sistemą
Įsibrovimai	Privilegijuotos paskyros sukompromitavimas
	Neprivilegijuotos paskyros sukompromitavimas
	Programos pažeidimas
Prieinamumas	DoS – paslaugų blokavimas
	DdoS – paskirstytas paslaugų blokavimas
	Sabotažas
Informacijos saugumas	Neteisėta prieiga prie informacijos
	Neteisėta informacijos modifikacija
Sukčiavimas	Neteisėtas išteklių naudojimas
	Autorinių teisių pažeidimas
	Apsimetinėjimas
Kita	Visi kiti incidentai, kurie nepaminėti šioje lentelėje



1.1 pav. „LITNET“ tinklo incidentų kiekis nuo 2016-01-01 iki 2017-05-02

1.1 paveiksle pavaizduota incidentų kiekis LITNET tinklo nuo 2016-01-01 iki 2017-05-02. Šiame paveiksle matome, kad didžiąją incidentų dalį sudaro sukčiavimas, toliau seka pažeidžiamumai ir žalingas kodas. Taip pat matosi, jog yra sutinkama ir kitų incidentų.

Pagal pateikta incidentų klasifikaciją ir „LITNET“ tinklo incidentų kiekį matome, jog problema tikrai egzistuoja ir reikalingos priemonės šiems incidentams suvaldyti, tam yra kuriami / naudojami aptikimo metodai. Aptikimo metodai gali būti automatizuoti aprašant žinomų atakų bruožus ar tinklo administratoriui stebint srautą / paslaugos veikimą turint didelę patirtį ir technines žinias, kuris pastebi nenormalų sistemos veikimą.

1.2. Incidentų kompiuterių tinkluose aptikimo metodai

Šiame skyriuje pateikiama informacija apie incidentų kompiuterių tinkluose aptikimo metodus.

Daugeliui organizacijų didžiausia iššūkio dalis, įvykus incidentui – tai nustatyti incidento tipą, mastą ir problemos dydį [2].

- incidentai gali būti aptikti tokiomis skirtingomis priemonėmis: automatizuotas aptikimas, antivirusinės programos ar žurnalų analizė. Incidentai taip pat gali būti aptinkami pasinaudojant kitų vartotojų praneštomis problemomis. Kai kurie incidentai turi atvirus žinomus ženklus, kurie gali būti lengvai aptinkami, tuo tarpu kiti yra beveik neaptinkami;
- specializuotos techninės žinios ir didelė patirtis yra būtinos norint atlikti efektyvią incidento duomenų analizę.

Įsibrovimo aptikimo sistema yra vienas iš incidentų aptikimo būdų ir klasifikuojama į dvi kategorijas [3]:

1) netinkamo naudojimo aptikimas (angl. *Misuse detection)* – sistema mokosi/apmokoma modelių iš jau žinomų atakų. Šie modeliai, per įeinančius duomenis, ieško įsibrovimų su jau žinomais ir apibrėžtais tipais. Šis metodas nesugeba aptikti naujų atakų, kurių modeliai nėra apibrėžti iš anksto;
2) anomalijos aptikimas – modeliai apibrėžti iš normalių duomenų. Nematyti duomenys patikrinami ir ieškoma nukrypimų pagal išmoktus modelius. Šie nukrypimai galimai įsibrovimas arba anomalija. Šis metodas nesugeba identifikuoti atakos tipo ir turi turėti visus galimus normalių duomenų atvejus. Duomenys turi būti išsamiai aprašyti, jog normalūs duomenys nebūtų identifikuoti kaip anomalija.

Incidentas – tai, fiksuotas rezultatas, pagal iš anksto žinomus saugos pažeidžiamumų atakų modelius. Anomalijos, iš anksto žinomų saugos pažeidžiamumų atakų modeliuose neatitikimai. Anomalija – nuokrypis nuo normos (norma – incidentą apibrėžiantis taisyklių rinkinys).

1.2.1. Tinklo anomalijų aptikimo metodai

Atrinkti metodai suskirstyti į statistinius, klasifikavimo, klasterizavimo ir taisyklių. Tinklo anomalijų aptikimo metodai [4] [5] [6]:

Statistinis metodas – tai metodas, pritaikantis statistinį modelį (paprastai normaliam elgesiui) į duotus duomenis ir tada taiko statistinį išvados testą, kad nustatytų ar nematytas atvejis priklauso šiam modeliui. Atvejai, kurie turi žemą tikimybę, laikomi anomalijomis. Anomalijoms aptikti suprojektuoti du metodai: parametrinė ir neparametrinė technika**.**

Statistinis anomalijų aptikimo metodas skirstomas į šiuos modelius:

- susimaišymo modelis (angl. *Mixture model*) – pagrįstas tuo, kad anomalija glūdi didelio normalių elementų skaičiaus viduje, *Eskin (2000)* pasiūlė susimaišymo modelį tam, kad aptiktų anomaliją triukšminguose duomenyse;
- signalo apdorojimo technika (angl. *Signal processing technique*) – pagrįsta staigiojo pasikeitimo susekimu. Apibrėžiamos dvi anomalijų rūšys:
    - anomalija atitinka tinklo įvykių nesėkmes ir atlikimo problemas;
    - apima susijusias su tokiomis saugumo svarstomomis problemomis, kaip paslaugos sutrikdymas – *DoS* atakos.

Statistinio metodo galimybės:

- nereikalauja išankstinių žinių apie įprastas tikslinės sistemos veiklas. Vietoje to, iš stebimo, turi gebėjimą išmokti tikėtiną sistemos veikimą;
- suteikia tikslius pranešimus arba perspėjimų generavimus apie kenkėjiškas veiklas atsitinkančias per ilgus laiko periodus, priklausomai nuo atitikimų nustatymų arba parametrų reguliavimo;
- analizuoja srautą remiantis netikėtų pokyčių teorija, t. y., ilgą laiką stebi srautą ir praneša, jei įvyko netikėtas pokytis (žymus nukrypimas).

Klasifikavimu grįstas metodas – tai metodas, kuris remiasi ekspertų žiniomis apie tinklo atakų charakteristikas. Tinklo ekspertas prideda į aptikimo sistemą žinomų atakų charakteristikas ir ataka su žinoma struktūra, gali būti aptikta jai vos tik prasidėjus. Ataka bus aptikta tik tuo atveju, jei tinklo ekspertas pateikė aprašą apie ataką, o nauja atakos rūšis, kuri neaprašyta, nebus aptikta.

Klasifikavimu grįstas metodas privalumai:

- yra lankstus apmokymams ir testavimams. Taipogi sugeba atnaujinti savo paleidimo strategijas įtraukiant naują informaciją. Todėl įmanomas pritaikomumas;
- turi aukštą aptikimo santykį žinomoms atakoms atitinkamam pradžios nustatymui.

Taisyklių metodas – naudojamas žinių sistemose. Sistemos administratorius sudaro taisykles, kuriomis gaunamos išvados apie neteisingą tinklo veikimą. Šiuo metodu sistemos gan lėtos ir priklauso

nuo sistemos administratoriaus kompetencijos ir teisingų taisyklių surašymo. Įvykus tinklo srauto pasikeitimui, o taisyklė nėra aprašyta šiam pasikeitimui, tokia anomalija nebus aptikta.

Taisyklių metodo privalumai:

- lanksčios ir užtikrintos;
- jei yra galimybė tinkamai surinkti pakankamai informacijos apie atakas ir įprastus atvejus, šis metodas turi didelį aptikimo santykį.

Klasterizavimo metodas – tai metodas, kai grupuojami panašūs duomenys į klasterius, nepriklausantys duomenys klasteriams laikomi nuokrypis nuo normos. Klasterizavimo metodas skirstomas į kontroliuojamus iš dalies ir nekontroliuojamus visiškai, metodus. Iš dalies kontroliuojamus įeina iš anksto sudaryti duomenys, kurie apibūdina normalų sistemos darbą. Nekontroliuojamas visiškai metodas – tai, kai atlikus panašių duomenų grupavimą į klasterius, reikia papildomo darbo įvertinti klasterių dydžiams ir atstumui tarp jų.

Klasterizavimo metodo privalumai:

- pavienis klasterizavimas yra efektyvus būdas greitam atsakymui generuoti;
- laipsniškam klasterizavimui (stebimame / prižiūrėtame rėžime) technikos yra efektyvios greitam atsakymų generavimui;
- palankus atvejais, kada grupuojami dideli duomenų rinkiniai į panašų kiekį klasių siekiant surasti tinklo anomalijas, nes tai sumažina skaičiavimo kompleksiškumą įsibrovimo aptikimo metu;
- suteikia stabilų veikimo našumą lyginant su klasifikavimo arba statistiniais metodais.

Atliktus tinklo anomalijų aptikimo metodų analizę, toliau bus analizuojama įsibrovimo aptikimo sistema. Įsibrovimo aptikimo sistemos pagrindiniai uždaviniai yra surinkti įvykius iš įvairių šaltinių, įvykių normalizacija, koreliacija, analizė ir sugeneruoti rezultatus:

Įvykių surinkimas iš įvairių šaltinių – pažeidžiamumų, kenkėjiškos veiklos, įtartinos veiklos ir kiti svarbūs duomenys, kurie yra operacinėse sistemose, apsaugos įrankiuose, tinklo srautuose. Visus šiuos duomenis stebėti atskirai yra problematiška, reikalauja daug laiko, daug išteklių, kenčia efektyvumas, laiku nepastebimi incidentai, anomalijos. Tam, kad laiku pastebėti ir reaguoti į incidentą ar anomaliją, efektyvesnis būdas visus duomenis surinkti į vieną sistemą ir joje stebėti.

Įvykių normalizacija – kiekviena sistema, turi savo žurnalinių įrašų saugojimo struktūrą. Todėl reikalingas įrankis kuris iš kiekvienos skirtingos sistemos įvykius sunormalizuotų ir išsiųstų į serverį, kuriame saugojama visa informacija apie įvykius, suprantama struktūra.

Koreliacija – įvykius koreliuojant iš įvairių šaltinių į vieną, galime gauti tikslesnę / naudingesnę informaciją apie įvykį.

Įvykio analizė – įsibrovimo aptikimo sistema kiekvieną gautą įvykį analizuoja, pagal serveryje aprašytas / patalpintas taisykles.

Įsibrovimo aptikimo sistemai, atlikus visus šiuos žingsnius sugeneruoja pranešimą / įspėjimą apie incidentą ar anomaliją.

1.2.2. Įsibrovimo aptikimo sistema

Įsibrovimas yra veiksmų šablonas, kuris sutrikdo kompiuterio saugumą ir tinklo komponentus konfidencialumo, vientisumo ir prieinamumo požiūriu. Tai gali būti atlikta vidaus ar išorės agento, kad gautų nesankcionuotą priėjimą prie saugumo ar įrenginio bei jo paslaugų mechanizmo kontrolės. Kad apsaugotų tinklo sistemų infrastruktūrą, įsibrovimo aptikimo sistemos (IDS) renka ir analizuoja, pagal šablonus informaciją iš įvairių šaltinių, jog identifikuotų galimus saugumo pažeidimus [7].

Įsibrovimo aptikimo funkcijas apima:

- stebimi ir analizuojami vartotojo veiksmai, sistema ir tinklo aktyvumas;
- konfigūruojama sistema, kad generuotų ataskaitas apie galimus pažeidžiamumus;
- vertinama sistemos ir failų vientisumas;
- atpažįstami žinomų atakų modeliai;
- analizuojama nenormali veikla;
- vartotojo taisyklių pažeidimų sekimas.

Įsibrovimų aptikimo sistema naudoja pažeidžiamumo vertinimą tam, kad įvertintų pagrindinio kompiuterio ar tinklo ir tinklo komponentų saugumą. Įsibrovimo aptikimo principas: įsibrovimo veikla yra pastebimai kitokia negu normalus sistemos veikimas arba atitinka žinomų atakų įvykių šablonus ir tokiu būdu aptinkamas [7].

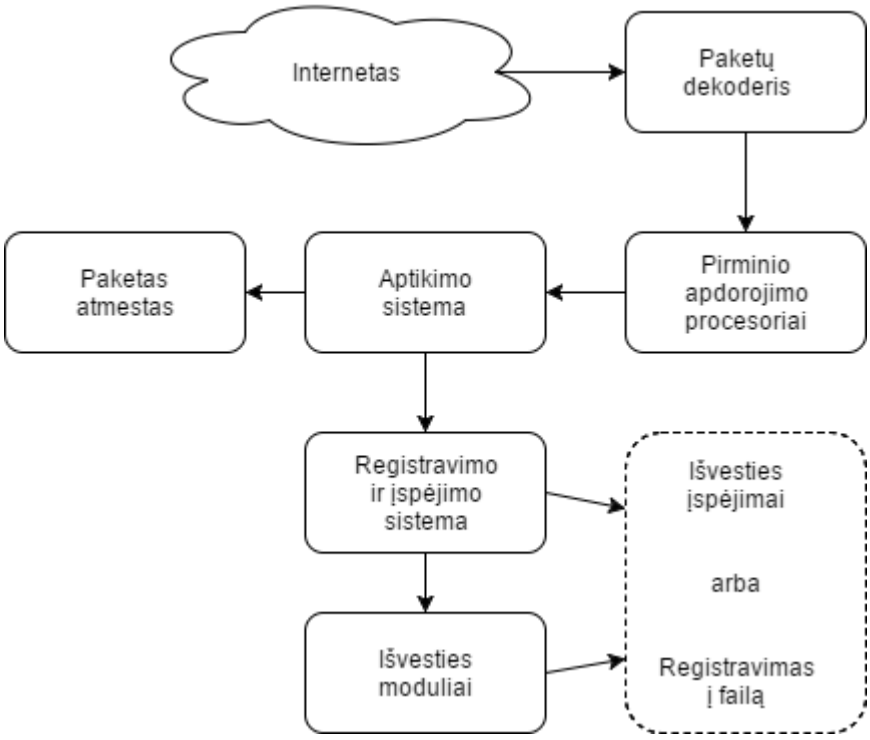
„Snort“ yra tinklo įsibrovimo aptikimo sistema NIDS, kuri skenuoja siunčiamus ir gaunamus paketus centralizuotuose pagrindinių tinklo paslaugų taškuose [8].

Įsibrovimo aptikimo sistemos nagrinėjamos pasirinktu „Snort“ sistemos pavyzdžiu.

„Snort“ yra logiškai suskirstyta į atskirus komponentus. Šie komponentai dirba kartu tam, kad aptiktų atakas ir sugeneruotų išvestis reikiamu formatu, kurio reikalauja aptikimo sistema [7].

„Snort „susideda iš šių pagrindinių komponentų [7]:

- paketų dekoderis (angl. *packet decoder*);
- pirminio apdorojimo procesoriai (angl. *Preprocessors*);
- aptikimo sistema;
- registravimo ir įspėjimo sistema;
- išvesties moduliai.



1.2 pav. Įsibrovimo aptikimo sistemos „Snort“ schema

„Snort“ komponentai yra išdėstyti taip, kaip pavaizduota 1.2 pav. [7].

Paketų dekoderis – identifikuoja gautų paketų protokolo tipą ir paruošia paketus pirminiam apdorojimui arba siunčia iškart į aptikimo sistemą.

Pirminio apdorojimo procesoriai – komponentai ar papildiniai, kurie gali būti panaudoti, kad sutvarkytų ar pakeistų duomenų paketus prieš jiems patenkant į susekimo sistemą, padarančią tam tikrą operaciją, jog sužinotų ar paketas yra naudojamas įsibrovėlio. Kai kurie pirminiai apdorojimo procesoriai taip pat įvykdo aptikimą, rasdami anomaliją paketo antraštėje, ir generuoja įspėjimą.

Aptikimo sistema – pati svarbiausia „Snort“ dalis. Sistemos tikslas aptikti, ar pakete egzistuoja kokia nors įsibrovimo veikla. Aptikimo sistema šiam tikslui naudoja „Snort“ taisykles.

Registravimo ir įspėjimo sistema – atsižvelgiant į tai, ką aptikimo sistemą rado pakete, paketas registruoja veiklą arba generuoja įspėjimą. Žurnalai laikomi paprastuose tekstiniuose failuose.

Išvesties moduliai(arba papildiniai) – gali daryti skirtingas operacijas. Iš esmės šie moduliai kontroliuoja sugeneruotą išvesties registravimo ir įspėjimo sistemą. Pranešimai gali būti siunčiami elektroninio pašto žinutėmis arba stebint įspėjimus tinklalapyje.

1.2.3. Kiti metodai

Failų vientisumo tikrinimo programinė įranga gali aptikti pakeitimus padarytus svarbiuose failuose. Naudoja maišos (angl. *hashing*) algoritmą, kad gautų šifruotą kontrolinę sumą kiekvienam failui. Jei failas yra pakeistas ir kontrolinė suma iš naujo apskaičiuota, didelė tikimybė, jog nauja sugeneruota kontrolinė suma neatitiks senos kontrolinės sumos. Reguliariai iš naujo apskaičiuodami

kontrolines sumas ir lygindami jas su ankstesnėmis kontrolinėmis sumomis, galime aptikti failų pasikeitimą ir taip identifikuoti grėsmę [6].

Aptikimas ne anomalijų ar įsibrovimo požymiu, bet neatitikimas numatytiems standartams (angl. *policies*), pvz.:

- nėra įdiegti paskutiniai pataisymai;
- esamas slaptažodis turi būti pakeistas pagal reikalavimus pasiekti informacijai;
- yra siunčiami į išorę vidiniai jautrūs dokumentai;
- naudojamas neregistruotas ar nenaudojantis duomenų šifravimo USB raktas.

Atlikus incidentų kompiuteriniuose tinkluose aptikimo metodų bei tinklo anomalijų aptikimo metodų ir įsibrovimo aptikimo sistemos analizę, toliau bus analizuojamos saugos informacijos įvykių valdymo ir saugojimo sistemos, kuriose yra šie įrankiai, kad būtų galima realizuoti mano kuriamą sistemą.

1.3. Saugos informacijos įvykių valdymo ir saugojimo sistemos

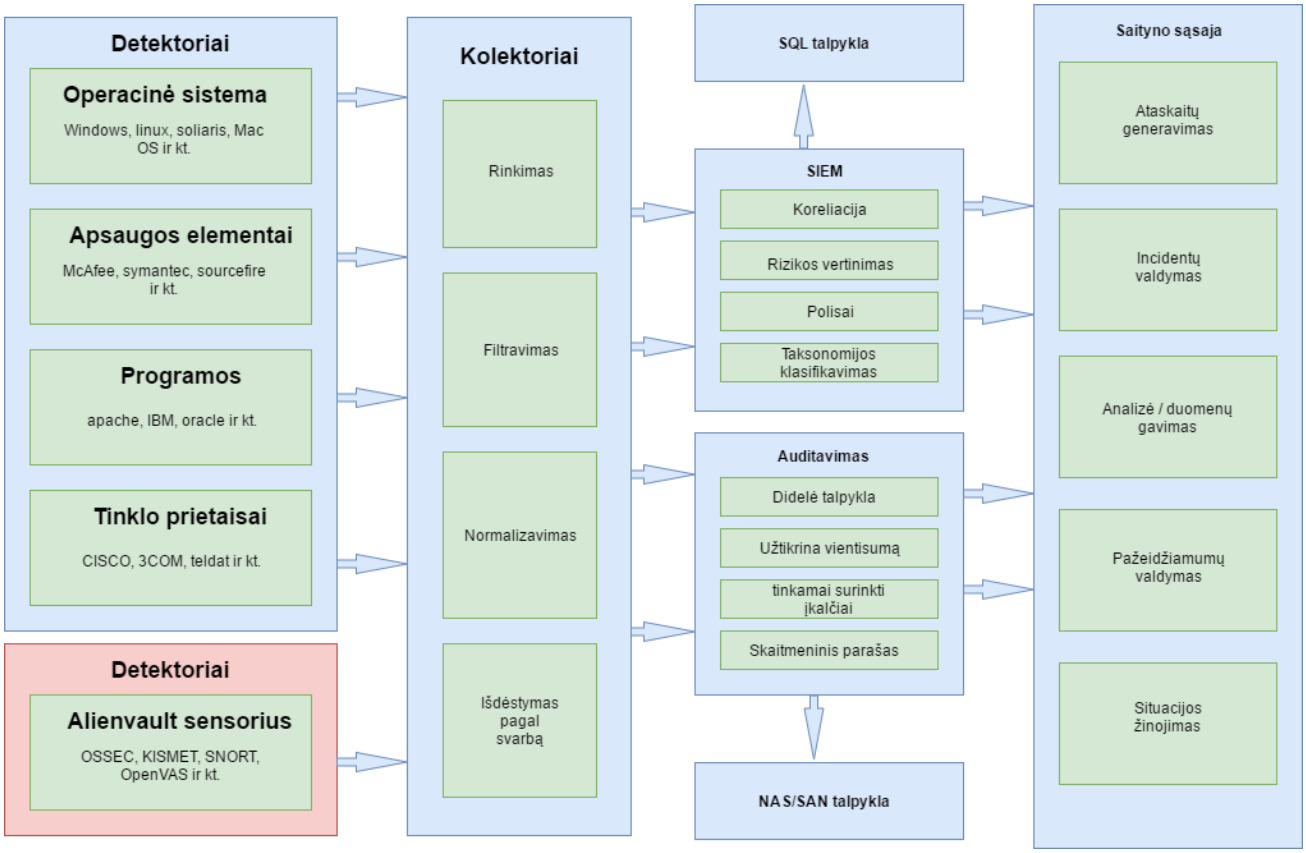
Analizuojant / renkantis saugos informacijos įvykių valdymo ir saugojimo sistemą, iškelti pagrindiniai kriterijai:

- įvykių normalizavimas – pasirinktoje saugos informacijos įvykių valdymo ir saugojimo sistemoje turi būti įvykių normalizavimas, kuris iš įvairių šaltinių gebėtų įvykius paversti į OSSIM serveriui suprantamą struktūrą;
- įsibrovimo aptikimo sistema „Snort“ – pasirinkta sistema turi gebėti palaikyti integruojamą komponentą „Snort“, kuris stebi ir analizuoja vartotojo veiksmus, sistemą ir tinklo aktyvumą, vertina sistemą ir failų vientisumą, atpažįsta žinomų atakų modelius, analizuoja nenormalią veiklą;
- pasirinkta sistema turi turėti saityno sąsają, kurioje administratorius galėtų valdyti incidentus, generuoti ataskaitas, stebėti ir valdyti pridėtus įrenginius;
- pasirinktoje sistemoje turi būti integruota atviro kodo apsauga OSSEC, renkanti informaciją iš pasirinktų šaltinių, kuriuose įdiegtas šis agentas, surinkęs informaciją apie sistemos veiklą, siunčia ją į pagrindinį serverį;
- programinės įrangos kaina – pasirinkta sistema turi būti atviro kodo, nieko nekainuoti.

Šiame skyriuje pateiksiu tris valdymo įrankius, pasirinktus pagal renginyje „SC Awards Europe 2016“ pristatytus geriausius SIEM sprendimus. Nugalėtoju tapo „Alienvault“ – vieningas saugumo valdymas (USM), taip pat aukštą įvertinimą gavo „Splunk“ – įmonės saugumas ir „IBM Security QRadar“.

Analizuojamos esamos sistemos pateiktos 1.3.1 – 1.3.3 poskyriuose.

1.3.1. „AlienVault“ – valdymo įrankis



1.3 pav. SIEM sistemos struktūra [9]

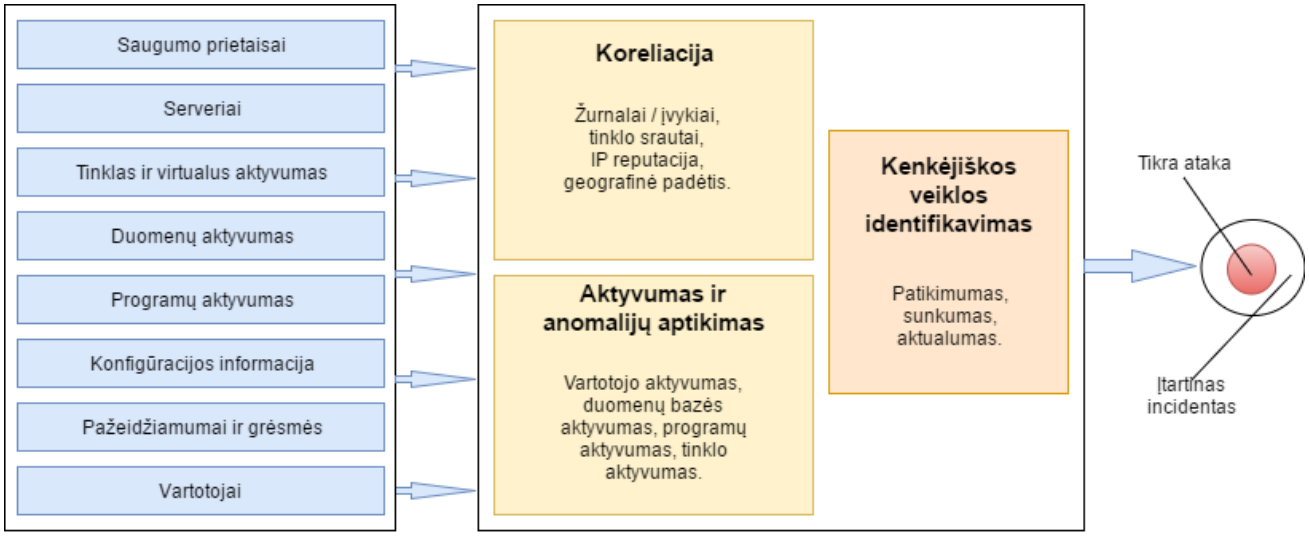
1.3 pav. pateikta SIEM sistemos struktūra. Šios sistemos struktūra susideda iš detektorių, kurie generuoja saugumo pažeidimo įvykius ir siunčia į kolektorius, kur vyksta įvykių rinkimas, filtravimas, normalizavimas ir išdėstymas pagal svarbą. Įvykiai įrašomi į talpyklas ir atvaizduojami saityno sąsajoje, kurioje galime generuoti ataskaitas, valdyti incidentus, gauti informaciją apie įvykio analizę ir valdyti pažeidžiamumus [9].

SIEM (Security information event management – informacijos saugumo ir įvykių valdymas), produkto galimybės rinkti, analizuoti ir pateikti informaciją iš tinklo, apsaugos prietaisų [9] [10].

Galimybės [10] [9] [11]:

- duomenų sujungimas – duomenys kaupiami iš daugelio šaltinių: tinklo, apsaugos programų, serverių, duomenų bazių, taikomųjų programų;
- koreliacija – ieškoma bendrų savybių iš įvykių, radus susiejama kartu. Ši technologija suteikia galimybę atlikti koreliaciją iš įvairių šaltinių, siekiant duomenis paversti į naudingą informaciją;
- įspėjimas – automatiškai siunčiami pranešimai gavėjui apie incidentą. Pranešimai gali būti įrašyti į valdymo sistemą / duomenų bazę arba siunčiami elektroniniai laiškai;
- valdymo sistema – įvykio duomenys sistemoje atvaizduojami diagramomis iš kurių galime matyti pokyčius ar pokytis virš reikalavimų ar ne.

1.3.2. „IBM Security QRadar“ – valdymo įrankis



1.4 pav. „IBM Security Qradar“ sistemos struktūra [12]

1.4 pav. pateikta „IBM Security Qradar“ sistemos struktūra. Šios sistemos struktūra susideda iš generuojamų / renkamų žurnalinių įrašų, įvykių. Taip pat yra vykdoma koreliacija pagal žurnalus / įvykius, tinklo srautus, IP reputaciją ir geografinę padėtį. Yra sekamas vartotojo, duomenų bazės, programų, tinklo aktyvumas. Toliau kenkėjiška veikla yra identifikuojama pagal tris kriterijus: patikimumą, sunkumą, aktualumą. Pabaigoje gauname rezultatą ar įvykęs incidentas yra tikra ataka ar tiesiog įtartinas incidentas.

“IBM Security's QRadar” saugumo tyrimų platformą apima: “QRadar SIEM”, anomalijų aptikimą, žurnalų valdymą, pažeidimų valdymą, rizikos valdymą, „QFlow“ ir „VFlow“ srautų surinkimą. Komponentai gali būti naudojami visi kartu (angl. *All-in-one*) arba atskirai [11].

„Qradar“ yra tinklo saugumo valdymo platforma, kuri suteikia informacijos apie situaciją ir suderinamumo palaikymą. „Qradar“ naudoja įvykių saugumo koreliaciją ir įrangos pažeidžiamumų vertinimą [12].

Žurnalų aktyvumas: „QRadar SIEM“ leidžia stebėti ir rodyti tinklo įvykius realiu laiku arba atlikti išplėstines paieškas [13].

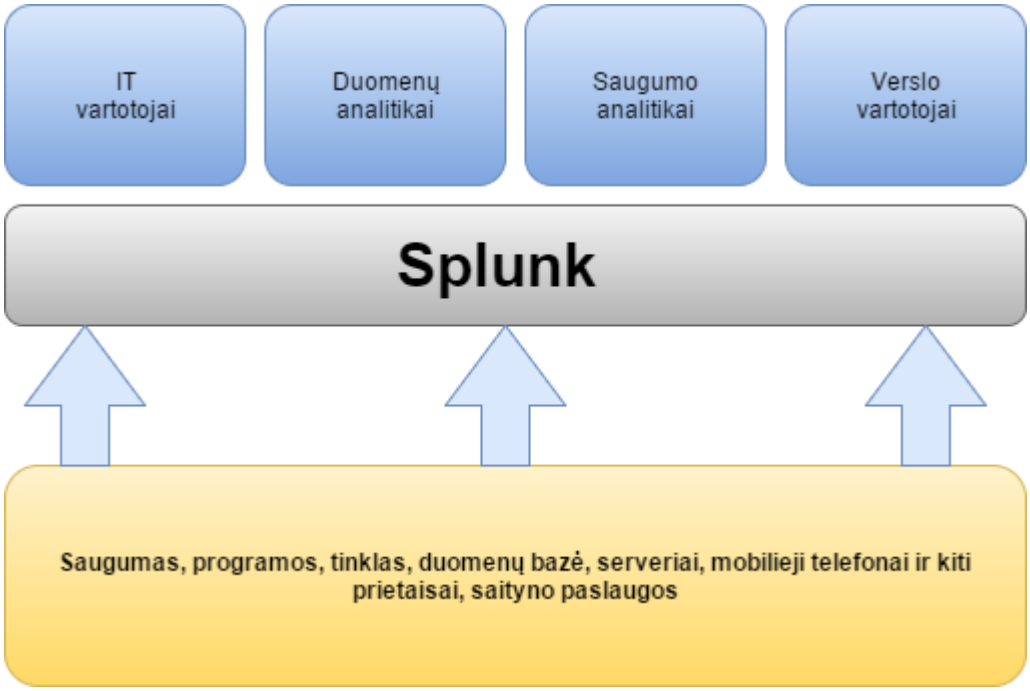
Tinklo aktyvumas: leidžia ištirti komunikacijos sesijas tarp dviejų pagrindinių kompiuterių [13].

Įranga: automatiškai susikuria įrangos profilis naudojant pasyvius srauto ir pažeidžiamumo duomenis tam, kad atrastų jūsų tinkle esančius serverius ir pagrindinius kompiuterius. Įrangos profiliai suteikia informaciją apie kiekvieną žinomą įrenginį jūsų tinkle, įskaitant veikiančias paslaugas. Įrangos profilio informacija naudojama koreliacijos tikslui – tam, kad sumažintų klaidingą informaciją [13].

Ataskaitos: leidžia kurti savo ataskaitas arba naudoti numatytąsias. Suteikia numatytuosius ataskaitų šablonus, kuriuos galima redaguoti ir platinti tarp vartotojų [13].

Duomenų rinkimas: informacija priimama įvairiais formatais ir iš įvairių prietaisų, įskaitant saugumo įvykius, tinklo srauto ir atlikto skenavimo rezultatus. Surinkti duomenys yra suskirstyti į tris kategorijas: įvykiai, srautai ir pažeidžiamumų vertinimo informacija [13].

1.3.3. „Splunk“ – valdymo įrankis



1.5 pav. „Splunk“ sistemos struktūra [14]

1.5 pav. pavaizduota „Splunk“ sistemos struktūra. Šios sistemos struktūra susideda iš gaunamų kompiuterinių, tinklo, duomenų bazių, mobiliųjų telefonų ir kitų prietaisų duomenų. Visa tai siunčiama į „Splunk“ serverį ir apdorojami gauti duomenys. „Splunk“ naudotojai yra IT vartotojai, duomenų analitikai, saugumo analitikai, verslo vartotojai.

„Splunk“ yra platforma kompiuteriniams duomenims. „Splunk Enterprise“ surenka visus kompiuterinius duomenis, kad ir kur jie sugeneruoti, įskaitant fizines, virtualias ir debesijos aplinkas. Taip pat leidžia ieškoti, stebėti ir analizuoti duomenis iš vienos vietos realiu laiku, išspręsti problemas ir ištirti saugumo incidentus per minutę, o ne valandomis ar dienomis [14].

Renkami ir indeksuojami bet kokie kompiuterio duomenys iš beveik bet kokio šaltinio, formato ar padėties, realiu laiku. Duomenys surenkami iš įsidiegtų programų, serverių, duomenų bazių, virtualių kompiuterių, mobiliųjų prietaisų, operacinių sistemų, jutiklių, centrinio kompiuterio ir kt. [14].

„Splunk“ savybės [15]:

- atranda automatiškai naudingą informaciją, nereikia ieškoti rankiniu būdu;
- konvertuoja žurnalų duomenis į vizualinius grafikus ir ataskaitas supaprastintai analizei;

- stebi sistemas ir infrastruktūras realiu laiku ir identifikuoja problemas anksčiau, nei jie paveikia jūsų verslą.

1.3.4. Įsibrovimo aptikimo sistemų apibendrinimas

1.2 lentelė Panašių sistemų palyginimo lentelė

Lyginimo kriterijai	**OSSIM**	**IBM security QRadar**	**Splunk**
Įvykių normalizavimas	Yra	Yra	Yra
Saityno sąsaja	Yra	Yra	Yra
Programinės įrangos kaina	Nemokama	Mokama	Mokama
Integruota programinė įranga (Snort, OSSEC)	yra	Nėra	Yra

1.2 lentelėje pateikiamas analizuotų sistemų palyginimas pagal nustatytus kriterijus. Atlikus panašių sistemų analizę ir lyginant jas su pasirinkta sistema, galime teigti, jog OSSIM geriausiai atitinka lyginimo kriterijus.

OSSIM yra atviro kodo, gebanti palaikyti tokias integruojamas programines įrangas, kaip „Snort“, „Suricata“, „OpenVas“, „Kismet“, „OSSEC“ visus šiuos įrangos komponentus sujungus į vieną bendrą sistemą, galime gauti panašų rezultatą, kaip ir mokamos sistemos, tokios kaip „Qrdar“ ir „Splunk“. Tačiau visa tai apjungti į vieną didelę veikiančią sistemą, reikalauja didelių techninių žinių. Šiame darbe bus bandoma patobulinti OSSIM valdymo įrankio efektyvumą, naudingumą, informatyvumą, pastebimumą pasinaudojant OSSEC agento galimybėmis.

1.4. Analizės išvados

Pateikti tinklo anomalijų aptikimo metodai: statistinis, klasifikavimu grįstas, taisyklėmis grįstas, klasterizavimo metodas.

Anomalijų aptikimas yra naudingas, nes tai palengvina sistemos / tinklo administratoriui suvaldyti, pastebėti ir reaguoti į incidentus.

Išanalizuota įsibrovimo aptikimo sistema remiantis OSSEC ir „Snort“ pavyzdžiu. Įsibrovimo aptikimo funkcijas apima: stebimi ir analizuojami vartotojo veiksmai, sistema ir tinklo aktyvumas; konfigūruojama sistema, kad generuotų ataskaitas apie galimus pažeidžiamumus; vertinama sistema ir failų vientisumas; atpažįstami žinomų atakų modeliai; analizuojama nenormali veikla; vartotojo taisyklių pažeidimų sekimas.

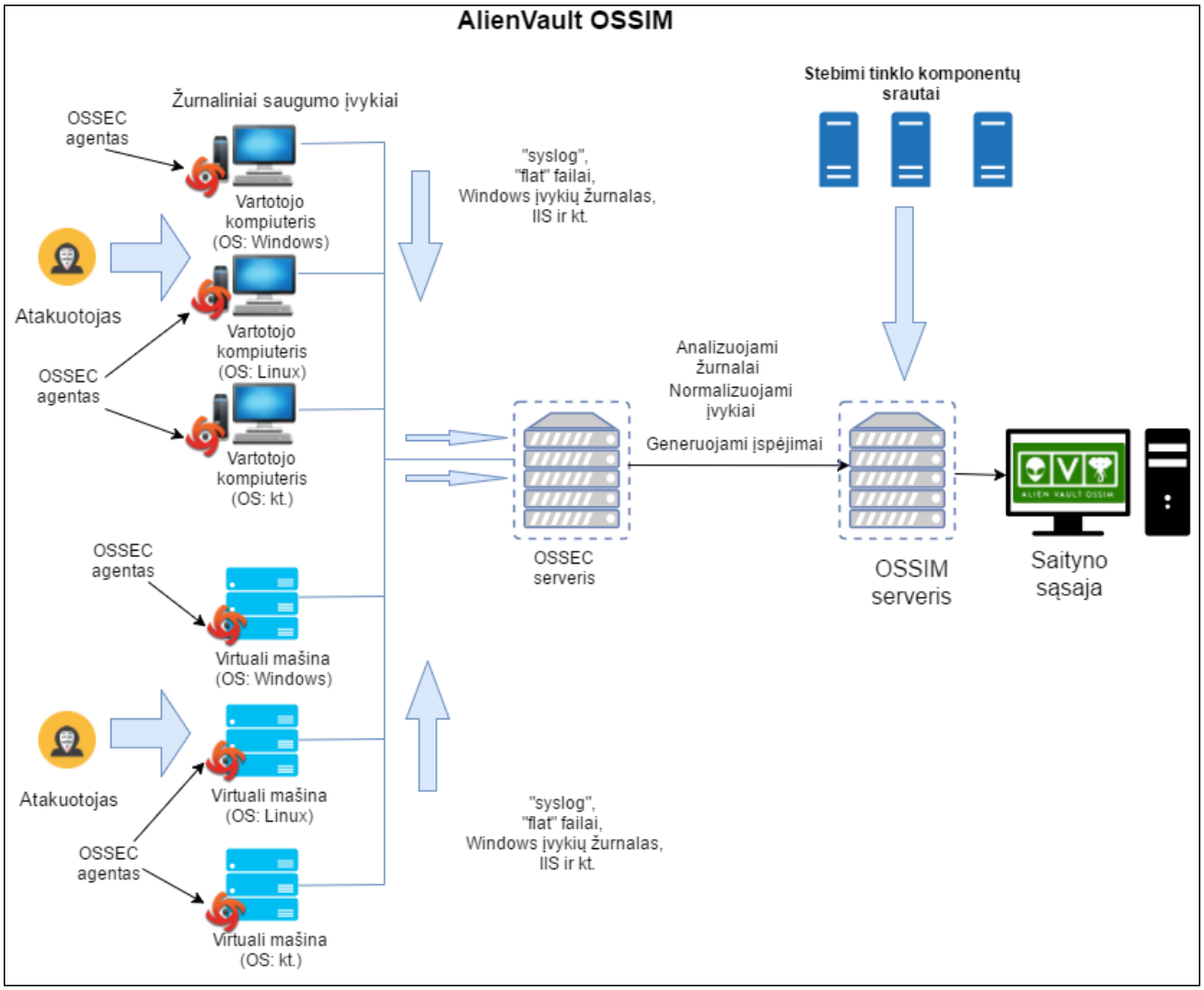
Pateiktos ir išanalizuotos panašios sistemos į pasirinktą, tad galime teigti, jog OSSIM geriausiai atitinka iškeltus lyginimo kriterijus. Todėl pasinaudojant OSSIM (Open source Security Information and Event management) platforma, bus įdiegiama realiu laiku veikianti sistema.

Šiame darbe bus bandoma patobulinti OSSIM valdymo įrankio efektyvumą, naudingumą, informatyvumą, pastebimumą pasinaudojant OSSEC agento galimybėmis. OSSEC agentu, OSSIM valdymo įrankyje, bus bandoma aprašyti metodus, kurie stebimose sistemose rinks informaciją apie aptiktas anomalijas.

2. INCIDENTŲ KOMPIUTERIŲ TINKLUOSE IDENTIFIKAVIMAS, TAIKANT ANOMALIJŲ APTIKIMO METODUS PROJEKTINĖ DALIS

Atlikus analizę kuriamas sistemos projektas jos realizacijai. Šiame skyriuje pateikiamos projektavimo stadijos ir detali projekto specifikacija. Sistema kuriama taip, kad atitiktų iškeltus reikalavimus.

Šios kuriamos sistemos tikslas: realiu laiku, automatiniu būdu aptikti anomalijas ir incidentus, realizacija atliekama OSSIM aplinkoje. Šios sistemos pagalba, tinklo administratorius gali lengviau identifikuoti ir reaguoti į incidentus.



2.1 pav. Bendra sistemos struktūra

Šiame 2.1 pav. pateikiamas bendras vaizdas kaip į OSSIM serverį atkeliauja žurnaliniai įvykiai. Atakuotojas, tai programišius, kuris bando pakenkti, kompromituoti sistemos veiklą.

OSSEC galimybės:

- žurnalų analizė, rinkimas, stebėjimas;
- failų vientisumo (angl. *integrity*) tikrinimas (Unix ir Windows);
- registrų vientisumo (angl. *integrity*) tikrinimas (Windows);

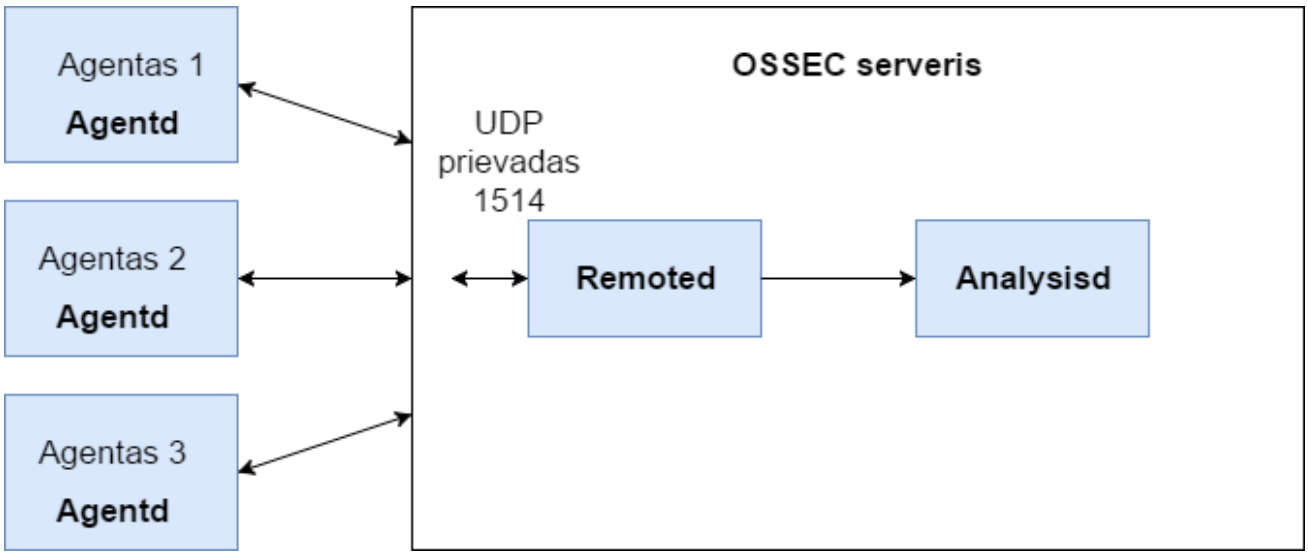
- pagrindinio kompiuterio (angl. *Host-based*) anomalijų aptikimas (Unix – rootkit aptikimas);
- aktyvus atsakas (angl. *active response*).

OSSIM serverio galimybės [9]:

- duomenų rinkimas ir normalizavimas – įvykiai yra renkami pagal „Snort“ taisykles iš pridėtų ir stebimų tinklo įrenginių, taip pat iš virtualių mašinų, kuriose įdiegtas OSSEC agentas;
- koreliacija – ieškoma bendrų savybių iš įvykių, radus susiejama kartu. Ši technologija suteikia galimybę atlikti koreliaciją iš įvairių šaltinių, siekiant duomenis paversti į naudingą informaciją;
- įspėjimas – automatiškai siunčiami pranešimai apie incidentą. Pranešimai gali būti įrašyti į valdymo sistemą ir / arba siunčiami elektroniniai laiškai;
- valdymo sistema – įvykio duomenys sistemoje atvaizduojami diagramomis, iš kurių galime matyti pokyčius, ar pokytis virš reikalavimų ar ne;
- rizikos vertinimas – formulę sudaro: įrenginio vertė, įvykio prioritetas ir įvykio patikimumas;
- duomenų analizė – atliekama gautų įvykių analizė pagal aprašytas taisykles.

Pirmiausia į virtualias mašinas, serverius, operacines sistemas, tokias kaip Microsoft Windows, „Linux“, „Soliaris“, „Mac OS“ ir kt. sistemas įdiegiami OSSEC (atviro kodo apsauga) agentai. Toliau atliekamas agento prijungimas / konfigūracija su serveriu ir taisyklių rašymas.

Komunikacija tarp OSSEC serverio ir virtualių mašinų, kuriose įdiegtas OSSEC agentas vyksta UDP protokolu ir prievadu 1514, kaip pavaizduota 2.2 pav. [16]:



2.2 pav. Komunikacija tarp kliento pusėje įdiegto agento ir OSSEC serverio

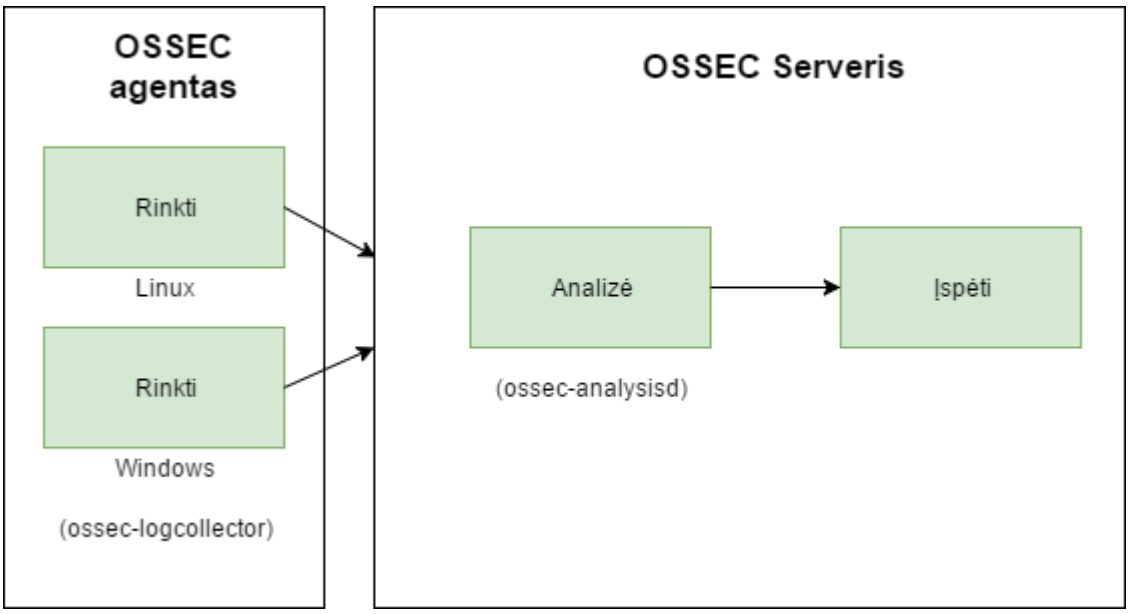
OSSEC serverį paleisti procesai:

- ossec-monitord – stebi agentų statusą, suspaudžia dienos žurnalinį failą;
- ossec-logcollector – skaito žurnalinius failus;
- ossec-remoted – priima žurnalus iš kliento, kuriame įdiegtas OSSEC agentas;
- ossec-syscheckd – tikrina konfigūruotus failus, teises ar nuosavybę;
- ossec-analysisd – pagrindinis procesas, kuris atlieka visą analizę.

Paleisti procesai virtualioje mašinoje, kurioje įdiegtas OSSEC agentas:

- ossec-logcollector – skaito žurnalinius failus;
- ossec-syscheckd – tikrina konfigūruotus failus, teises ar nuosavybę;
- ossec-agentd – siunčia žurnalus į OSSEC serverį;
- ossec-execd – vykdo aktyvius atsakymus.

Bendras vaizdas koks procesas renka žurnalinius įrašus ir koks procesas analizuoja [16]:



2.3 pav. OSSEC agentas siunčia surinktus duomenis į OSSEC serverį

2.3 pav. pavaizduota, kaip OSSEC agento procesas *ossec-logcollector*, kuris įdiegtas virtualiose mašinose „Windows“ ir „Linux“, renka informaciją apie virtualias mašinas ir siunčia surinktą informaciją į OSSEC serverį, kuriame paleistas pagrindinis procesas *ossec-analysisd*, atliekantis visą svarbiausią įvykio analizę;

OSSEC agentas „Linux“ virtualioje mašinoje stebi šiuos žurnalinius failus:

- /var/log/messages;
- /var/log/auth.log;
- /var/log/syslog;
- /var/log/mail.info;
- /var/log/dpkg.log;
- /var/log/apache2/error.log;
- /var/log/apache2/access.log.

OSSEC agentas realiu laiku stebi failų pasikeitimus šiuose kataloguose:

- /var/www/html – „Linux“ virtuali mašina;
- C:\Users\povilas\Desktop\Security – „Windows“ virtuali mašina.

Windows virtualioje mašinoje įdiegto OSSEC agentas renka duomenis iš šių įvykių grupių [17]:

- „Application“ – bet kokios programų klaidos fiksuojamos kaip įvykis;
- „security“ – saugumo įvykiai; orientuota į bandymus prisijungti prie operacinės sistemos;
- „system“ – bet kokia sistemos nesėkmė turi būti stebima ir fiksuojama;
- „Windows PowerShell“ – stebima „PowerShell“ veikla.

Aprašytos taisyklės bilietų (angl. *tickets*) kūrimui. Šiuo metu kuriami įvykių bilietai pagal šias išvardintas taisykles:

- failų vientisumo pasikeitimas;
- failas pridėtas į sistemą;
- OSSEC agentas atsijungė nuo sistemos;
- OSSEC agentas pradėjo savo darbą;
- naujų prievadų statusų pasikeitimas.

2.1. Funkciniai reikalavimai

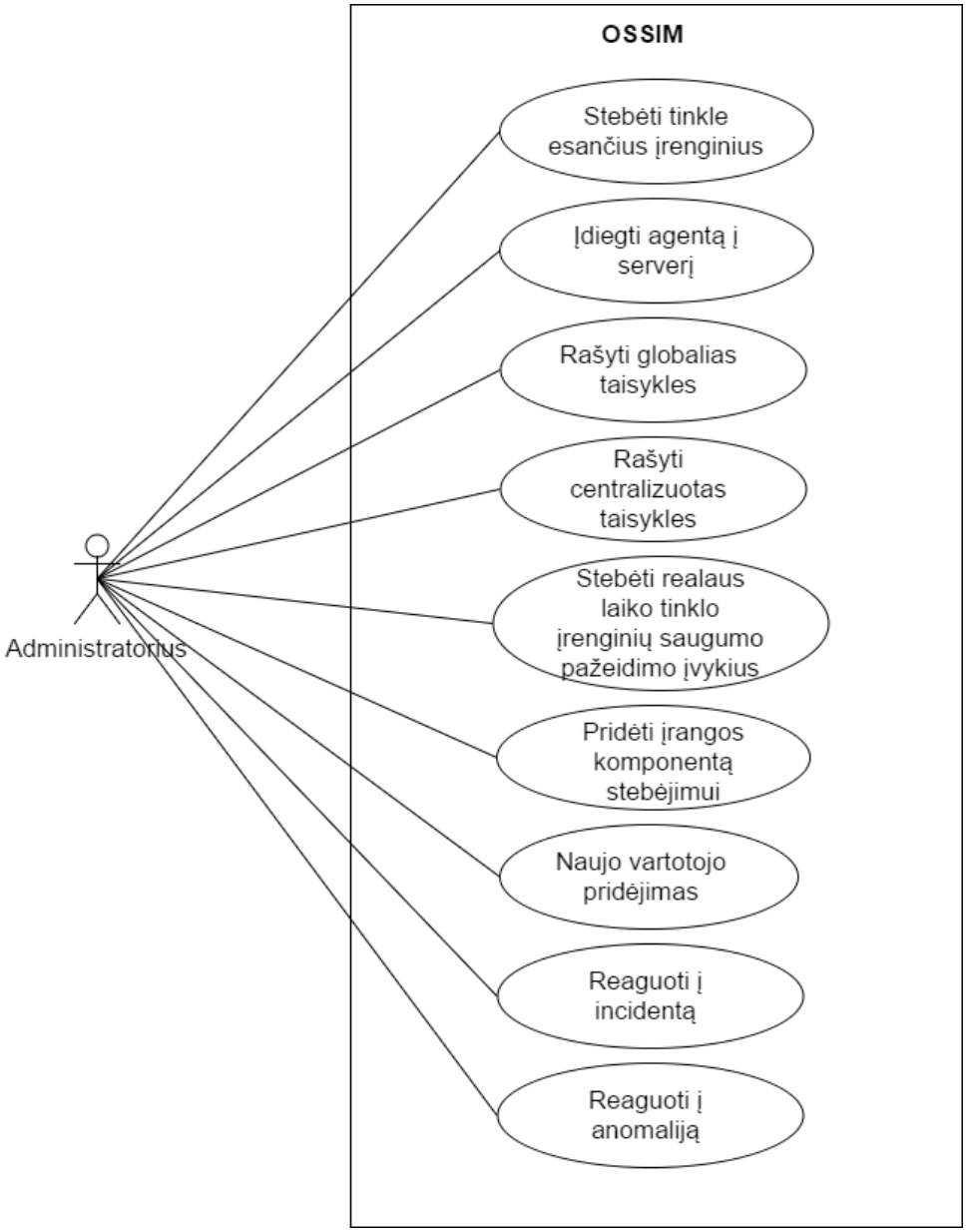
Prieš pateikiant aiškiai suformuluotus funkcinius reikalavimus kuriamam produktui ir sudarant panaudos atvejus, reikia apsirašyti kuriamos sistemos aktorius. Kuriamojoje sistemoje yra du aktoriai:

Administratorius – kuriamos sistemos aktorius, kuris naudojasi kuriama sistema identifikavimui ir reagavimui į incidentus.

Sistema – aktorius, kuris gauna visą informaciją iš serverių, ją apdoroja ir normalizuoja.

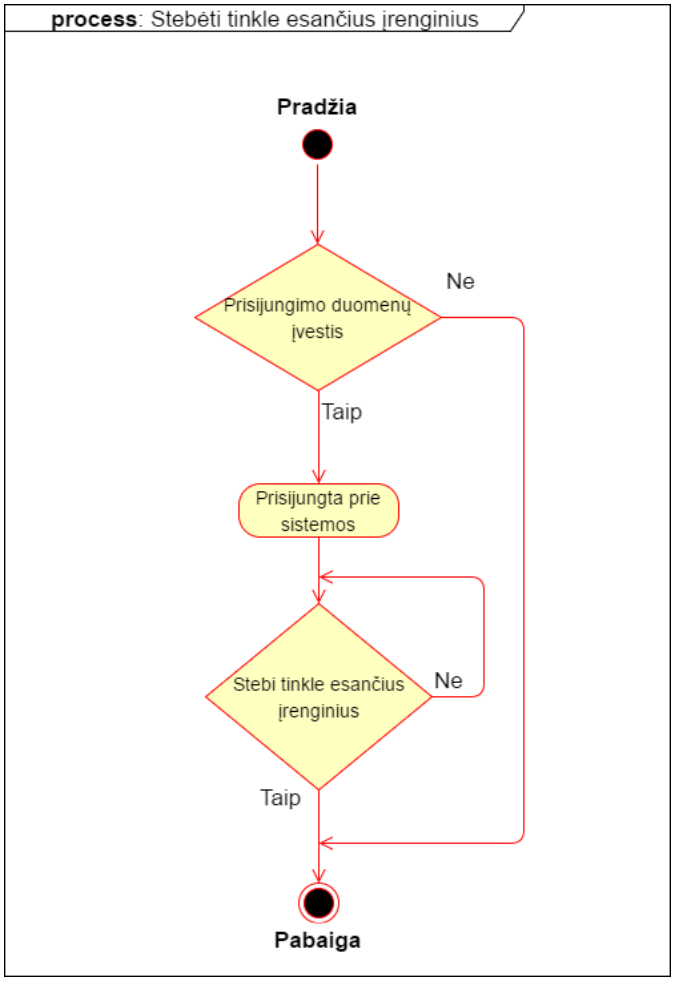
Administratoriaus panaudos atvejo diagrama pateikta 2.4 pav.

Sistemos panaudos atvejo diagrama pateikta 2.14 pav.



2.4 pav. Administratoriaus panaudos atvejų diagrama

2.5 pav. pavaizduota, kaip administratorius, prisijungęs prie sistemos, stebi tinkle esančius įrenginius. Pirmiausia administratorius turi įvesti prisijungimo duomenis, jog prisijungtų prie sistemos. Jei prisijungimo duomenys teisingi ir sistema pilnai funkcionuoja, administratorius prisijungia prie sistemos ir stebi tinkle esančius įrenginius. Administratorius nemato tinkle esančių įrenginių, jeigu nėra įtrauktų į tinklą įrenginių.



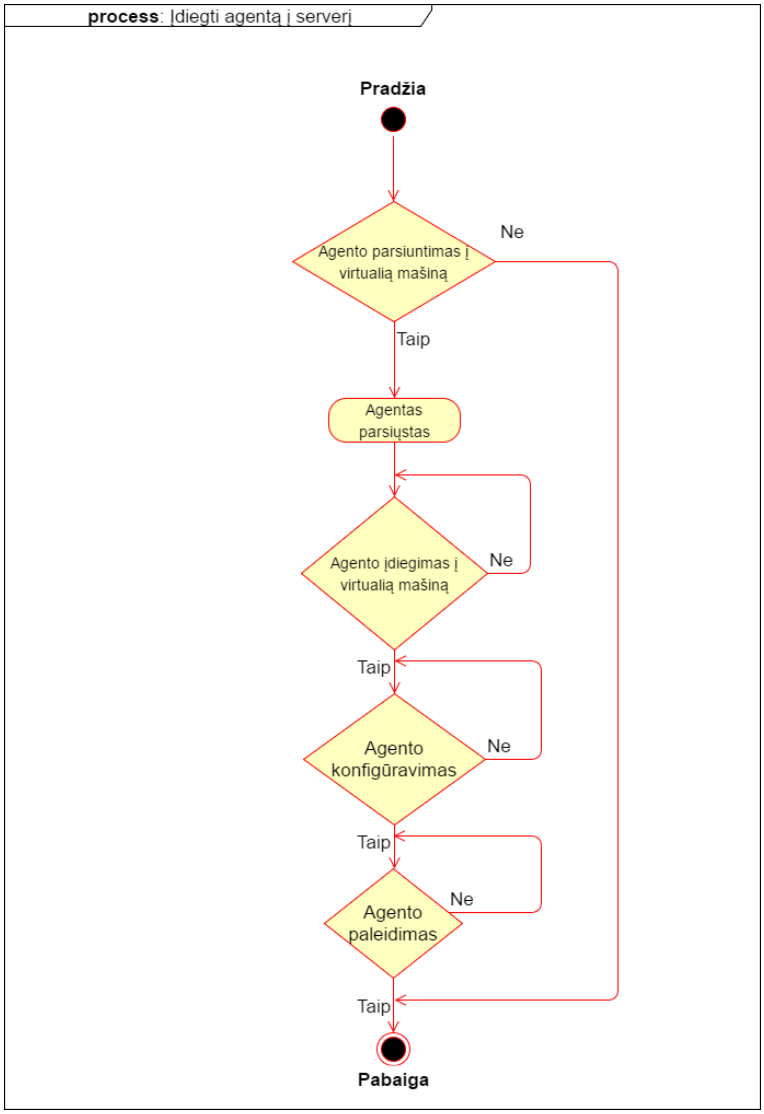
2.5 pav. Stebėjimo tinkle esančių įrenginių veiklos diagrama

Administratoriaus stebėjimo tinkle esančių įrenginių panaudos atvejo aprašymas pateiktas 2.1 lentelėje.

2.1 lentelė Stebėjimo tinkle esančių įrenginių panaudos atvejo aprašymo lentelė

ID	PA-01
Pavadinimas	Stebėti tinkle esančius įrenginius
Aprašymas	Administratorius OSSIM aplinkoje gali stebėti, kokie įrenginiai yra tinkle.
Aktoriai	Administratorius
Pradinės sąlygos	Administratorius turi prisijungti prie sistemos. Turi būti pridėti įrenginiai.
Pagrindiniai žingsniai	Administratorius prisijungia prie sistemos ir stebi tinkle esančius įrenginius.
Išskirtinės situacijos	Sistema neveikia, nėra tinkle įrenginių.
Galutinės sąlygos	Stebi tinkle esančius įrenginius.

2.6 pav. pavaizduotas agento diegimas į serverį ar virtualią mašiną. Pirmiausia administratorius turi parsiųsti agentą į serverį ar virtualią mašiną. Tuomet administratorius atlieka agento diegimą ir konfigūravimą serveryje ar virtualioje mašinoje.



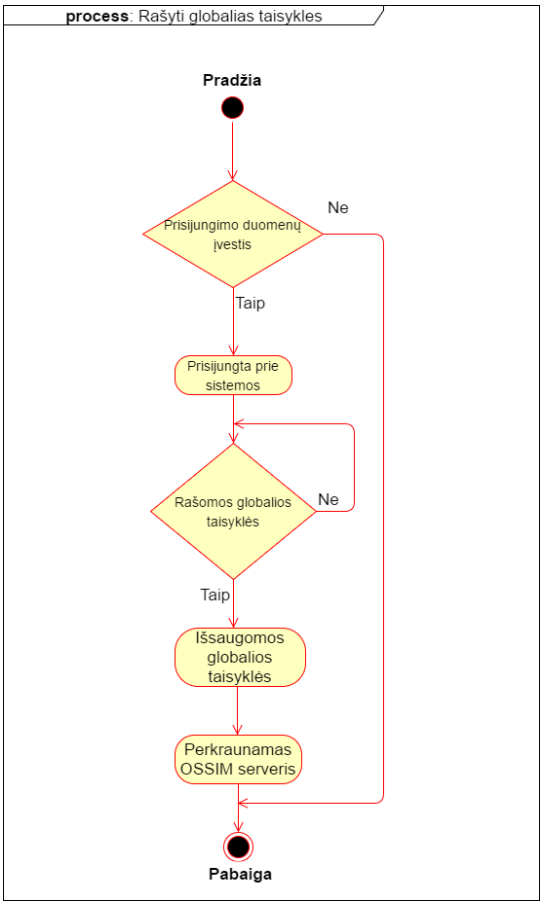
2.6 pav. Agento diegimo į serverį veiklos diagrama

Agento diegimo į serverį panaudos atvejo aprašymas pateiktas 2.2 lentelėje.

2.2 lentelė agento diegimo į serverį panaudos atvejo aprašymo lentelė

ID	PA-02
Pavadinimas	Įdiegti agentą į serverį
Aprašymas	Administratorius įdiegia agentą į virtualią mašiną tam, jog siųstų į OSSIM aplinką žurnalinius įrašus.
Aktoriai	Administratorius
Pradinės sąlygos	Įdiegia agentą į virtualią mašiną.
Pagrindiniai žingsniai	Parsiunčiamas OSSEC agentas į virtualią mašiną, tuomet įdiegiamas agentas, konfigūruojamas ir paleidžiamas.
Išskirtinės situacijos	Nepavyksta parsiųsti agento į virtualią mašiną.
Galutinės sąlygos	Parsiunčiamas agentas į virtualią mašiną ir sėkmingai įdiegiamas. Žurnaliniai įrašai siunčiami į OSSIM aplinką.

2.7 pav. pavaizduota, kaip administratorius, prisijungęs prie sistemos, rašo globalias taisykles. Pirmiausia administratorius turi įvesti prisijungimo duomenis, jog prisijungtų prie sistemos. Jei prisijungimo duomenys yra teisingi ir sistema pilnai funkcionuoja, administratorius prisijungia prie sistemos ir rašo globalias taisykles. Parašęs globalias taisykles administratorius jas išsaugo ir perkrauna OSSIM serverį. Administratorius negali rašyti globalių taisyklių, jeigu nėra įdiegtų agentų į serverį ar virtualią mašiną.



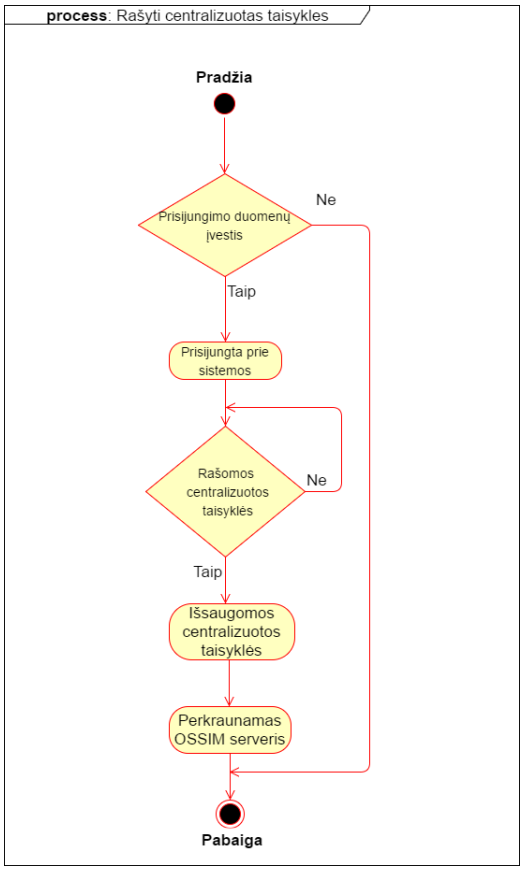
2.7 pav. Globalių taisyklių rašymo veikos diagrama

Globalių taisyklių rašymo panaudos atvejo aprašymas pateiktas 2.3 lentelėje.

2.3 lentelė Globalių taisyklių rašymo panaudos atvejo aprašymo lentelė

ID	PA-03
Pavadinimas	Rašyti globalias taisykles
Aprašymas	Administratorius gali rašyti taisykles, kurios gali būti taikytinos visoms pridėtoms virtualioms mašinoms.
Aktoriai	Administratorius
Pradinės sąlygos	Administratorius turi prisijungti prie sistemos.
Pagrindiniai žingsniai	Administratorius rašo globalias taisykles. Tuomet jas išsaugo ir perkrauna OSSIM serverį.
Išskirtinės situacijos	Sistema neveikia. Nėra pridėtų įrenginių.
Galutinės sąlygos	Generuojami nauji įvykiai pagal aprašytas globalias taisykles.

2.8 pav. pavaizduota, kaip administratorius, prisijungęs prie sistemos, rašo centralizuotas taisykles. Pirmiausia administratorius turi įvesti prisijungimo duomenis, jog prisijungtų prie sistemos. Jei prisijungimo duomenys teisingi ir sistema pilnai funkcionuoja, administratorius prisijungia prie sistemos ir rašo centralizuotas taisykles. Parašęs centralizuotas taisykles administratorius jas išsaugo ir perkrauna OSSIM serverį. Administratorius negali rašyti centralizuotų taisyklių, jeigu nėra įdiegtų agentų į serverį ar virtualią mašiną.



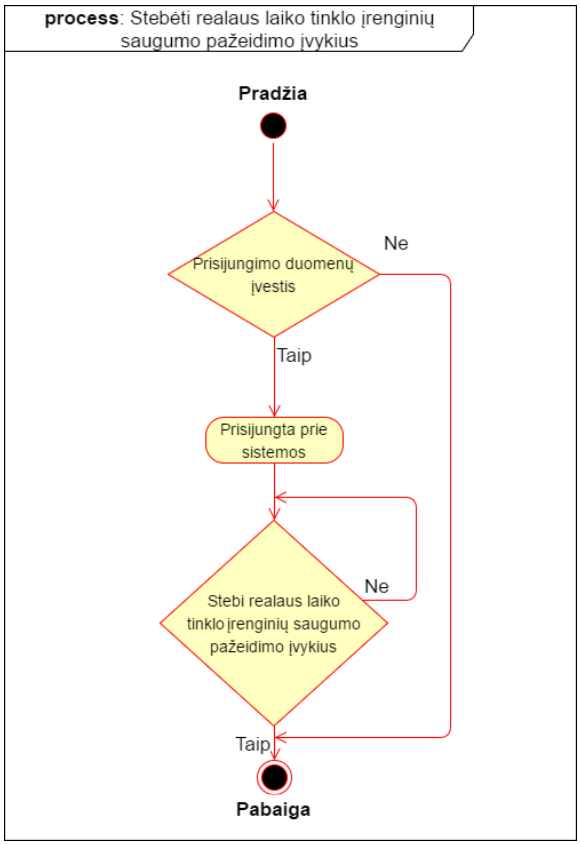
2.8 pav. Centralizuotų taisyklių rašymo veiklos diagrama

Centralizuotų taisyklių rašymo panaudos atvejo aprašymas pateiktas 2.4 lentelėje.

2.4 lentelė Centralizuotų taisyklių rašymo panaudos atvejo aprašymo lentelė

ID	PA-04
Pavadinimas	Rašyti centralizuotas taisykles
Aprašymas	Administratorius gali rašyti taisykles, kurios gali būti taikytinos tik pasirinktam įrenginiui.
Aktoriai	Administratorius
Pradinės sąlygos	Administratorius turi prisijungti prie sistemos.
Pagrindiniai žingsniai	Administratorius rašo centralizuotas taisykles. Tuomet jas išsaugo ir perkrauna OSSIM serverį.
Išskirtinės situacijos	Sistema neveikia. Nėra pridėto įrenginio.
Galutinės sąlygos	Generuojami nauji įvykiai pagal aprašytas centralizuotas taisykles.

2.9 pav. pavaizduota, kaip administratorius, prisijungęs prie sistemos, stebi realaus laiko tinklo įrenginių saugumo pažeidimo įvykius. Pirmiausia administratorius turi įvesti prisijungimo duomenis, jog prisijungtų prie sistemos. Jei prisijungimo duomenys teisingi ir sistema pilnai funkcionuoja, administratorius prisijungia prie sistemos ir stebi realaus laiko tinklo įrenginių saugumo pažeidimo įvykius. Administratorius negali stebėti realaus laiko tinklo įrenginių saugumo pažeidimo įvykių, jeigu tinkle nėra įrenginių.



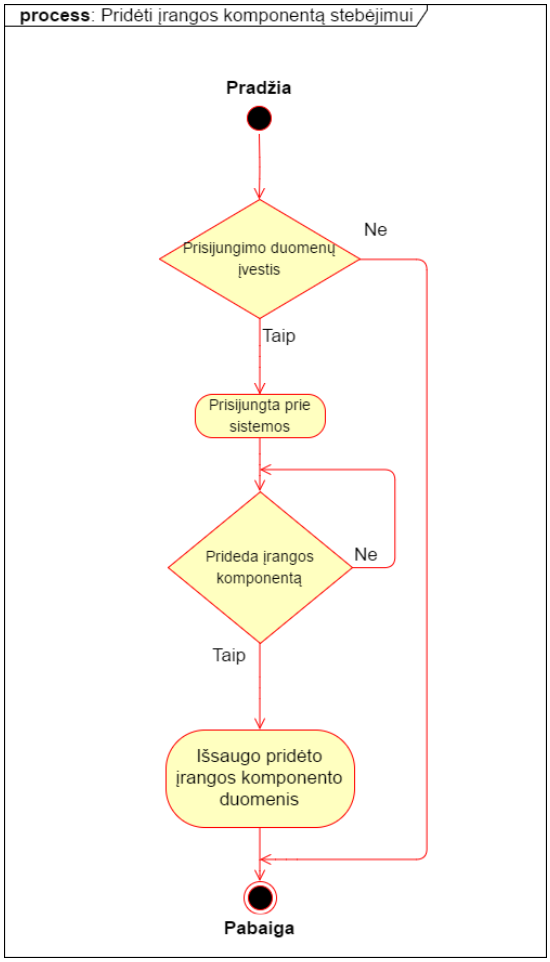
2.9 pav. Realaus laiko tinklo įrenginių saugumo pažeidimo įvykių stebėjimo veiklos diagrama

Realaus laiko tinklo įrenginių saugumo pažeidimo įvykių stebėjimo panaudos atvejo aprašymas pateiktas 2.5 lentelėje.

2.5 lentelė Realaus laiko tinklo įrenginių saugumo pažeidimo įvykių stebėjimo panaudos atvejo aprašymo lentelė

ID	PA-05
Pavadinimas	Stebėti realaus laiko tinklo įrenginių saugumo pažeidimo įvykius
Aprašymas	Administratorius OSSIM aplinkoje gali stebėti realaus laiko tinklo įrenginių saugumo pažeidimo įvykius.
Aktoriai	Administratorius
Pradinės sąlygos	Administratorius turi prisijungti prie sistemos.
Pagrindiniai žingsniai	Administratorius prisijungia prie sistemos ir stebi realaus laiko tinklo įrenginių saugumo pažeidimo įvykius.
Išskirtinės situacijos	Sistema neveikia, nėra tinkle įrenginių.
Galutinės sąlygos	Stebi realaus laiko tinklo įrenginių saugumo pažeidimo įvykius.

2.10 pav. pavaizduota, kaip administratorius, prisijungęs prie sistemos, prideda įrangos komponentą stebėjimui. Pirmiausia administratorius turi įvesti prisijungimo duomenis, jog prisijungtų prie sistemos. Jei prisijungimo duomenys teisingi ir sistema pilnai funkcionuoja, administratorius prisijungia prie sistemos ir prideda įrangos komponentą stebėjimui. Administratorius negali pridėti įrangos komponento stebėjimui, jeigu sistema neveikia.



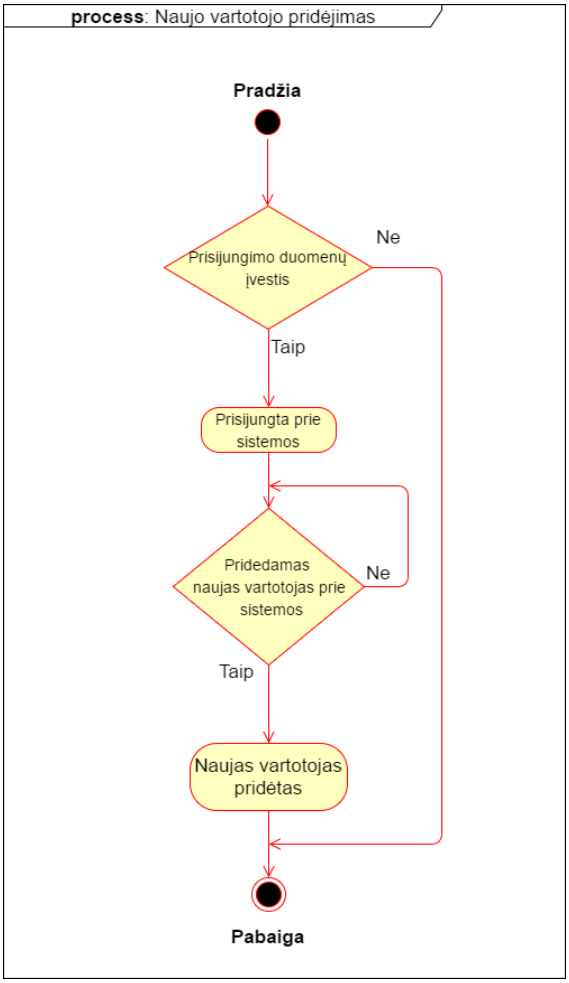
2.10 pav. Įrangos komponento pridėjimas stebėjimui veiklos diagrama

Įrangos komponento pridėjimas stebėjimui panaudos atvejo aprašymas pateiktas 2.6 lentelėje.

2.6 lentelė Įrangos komponento pridėjimas stebėjimui panaudos atvejo aprašymo lentelė

ID	PA-06
Pavadinimas	Pridėti įrangos komponentą stebėjimui
Aprašymas	Administratorius gali pridėti įrangos komponentą ir stebėti įvykius iš jo.
Aktoriai	Administratorius
Pradinės sąlygos	Administratorius turi prisijungti prie sistemos.
Pagrindiniai žingsniai	Administratorius prisijungia prie sistemos ir prideda įrangos komponentą.
Išskirtinės situacijos	Sistema neveikia.
Galutinės sąlygos	Pridedamas įrangos komponentas ir stebimi įvykiai iš jo.

2.11 pav. pavaizduota, kaip administratorius, prisijungęs prie sistemos, prideda naują vartotoją. Pirmiausia administratorius turi įvesti prisijungimo duomenis, jog prisijungtų prie sistemos. Jei prisijungimo duomenys teisingi ir sistema pilnai funkcionuoja, administratorius prideda naują vartotoją prie sistemos. Administratorius negali pridėti įrangos komponento stebėjimui, jeigu sistema neveikia.



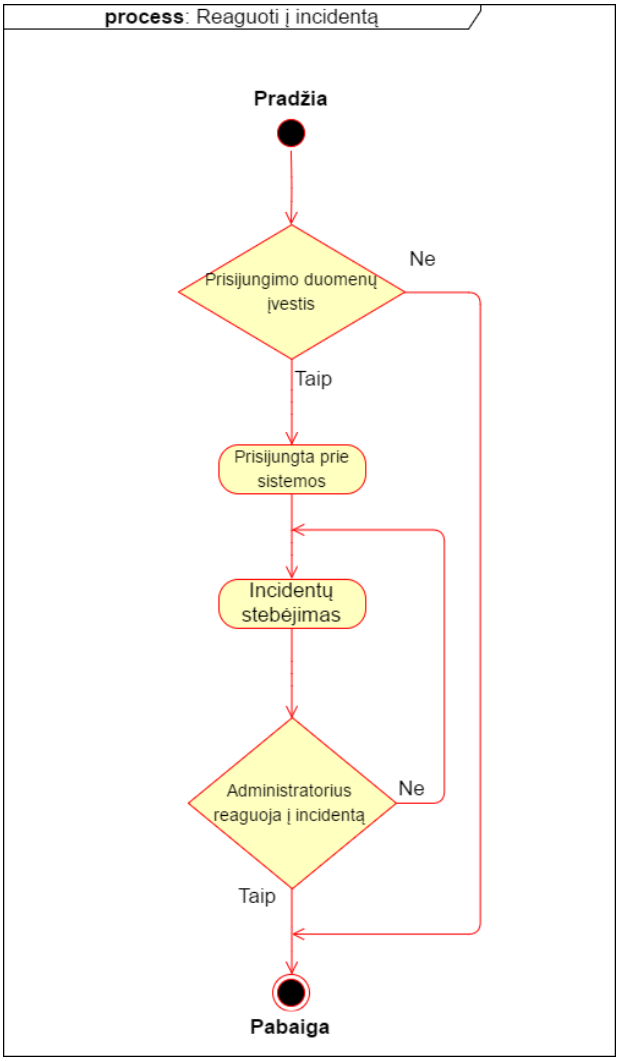
2.11 pav. Naujo vartotojo pridėjimo veiklos diagrama

Naujo vartotojo pridėjimo panaudos atvejo aprašymas pateiktas 2.7 lentelėje.

2.7 lentelė Naujo vartotojo pridėjimo panaudos atvejo aprašymo lentelė

ID	PA-07
Pavadinimas	Naujo vartotojo pridėjimas
Aprašymas	Administratorius gali pridėti naują vartotoją prie sistemos
Aktoriai	Administratorius
Pradinės sąlygos	Administratorius turi prisijungti prie sistemos.
Pagrindiniai žingsniai	Administratorius prisijungia prie sistemos ir prideda naują vartotoją prie sistemos.
Išskirtinės situacijos	Sistema neveikia.
Galutinės sąlygos	Pridedamas naujas vartotojas prie sistemos

2.12 pav. pavaizduota, kaip administratorius, prisijungęs prie sistemos, reaguoja į incidentą. Pirmiausia administratorius turi įvesti prisijungimo duomenis, jog prisijungtų prie sistemos. Jei prisijungimo duomenys teisingi ir sistema pilnai funkcionuoja, administratorius stebi incidentus ir reaguoja į juos. Administratorius negali stebėti incidentų, jeigu sistema neveikia ir nėra incidentų.



2.12 pav. Reagavimo į incidentą veiklos diagrama

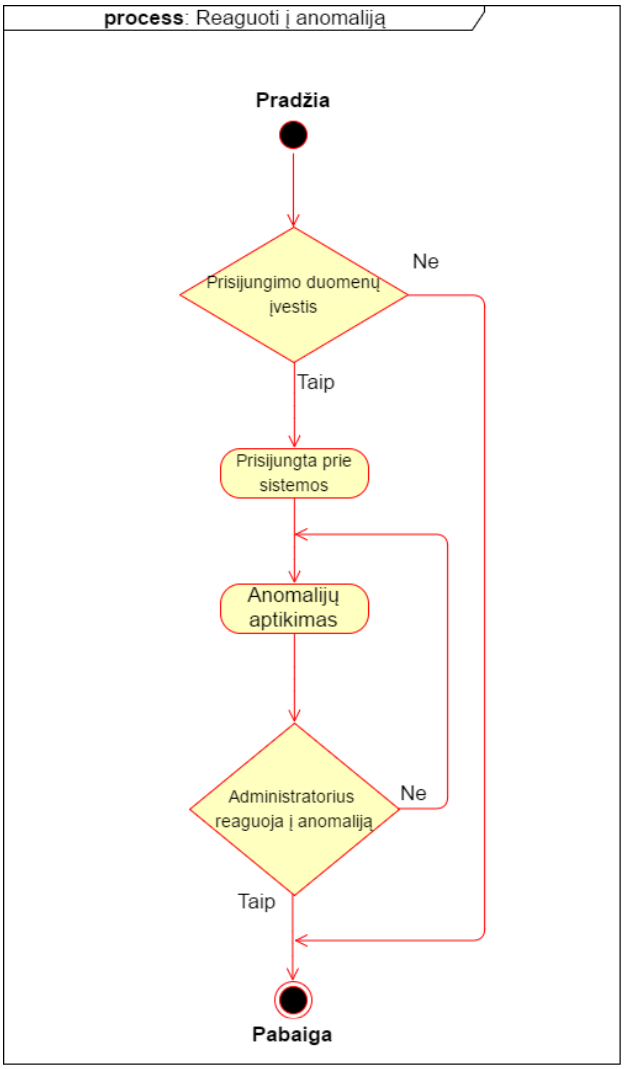
Reagavimo į incidentą panaudos atvejo aprašymas pateiktas 2.8 lentelėje.

2.8 lentelė Reagavimo į incidentą panaudos atvejo aprašymo lentelė

ID	PA-08
Pavadinimas	Reaguoti į incidentą
Aprašymas	Administratorius reaguoja į incidentą (fiksuotas rezultatas, pagal iš anksto sudarytas taisykles).
Aktoriai	Administratorius
Pradinės sąlygos	Administratorius turi prisijungti prie sistemos.
Pagrindiniai žingsniai	Administratorius prisijungia prie sistemos ir reaguoja į incidentą
Išskirtinės situacijos	Sistema neveikia. Nėra incidentų.
Galutinės sąlygos	Administratorius reaguoja į incidentą.

2.13 pav. pavaizduota, kaip administratorius, prisijungęs prie sistemos, reaguoja į anomaliją. Pirmiausia administratorius turi įvesti prisijungimo duomenis, jog prisijungtų prie sistemos. Jei

prisijungimo duomenys teisingi ir sistema pilnai funkcionuoja, administratorius aptinka anomaliją ir reaguoja į ją. Administratorius negali aptikti anomalijų, jeigu sistema neveikia ir nėra anomalijų.

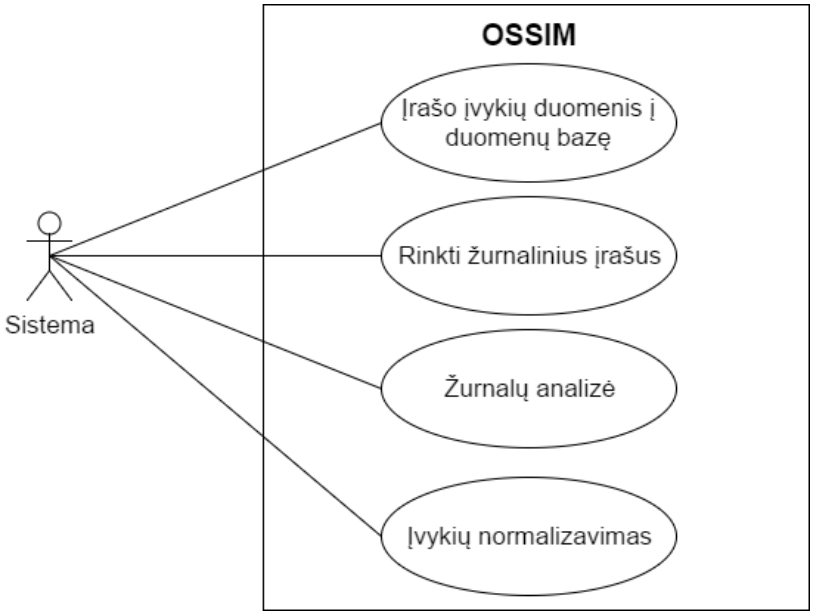


2.13 pav. Reagavimo į anomaliją veiklos diagrama

Reagavimo į anomaliją panaudos atvejo aprašymas pateiktas 2.9 lentelėje.

2.9 lentelė Reagavimo į anomaliją panaudos atvejo aprašymo lentelė

ID	PA-09
Pavadinimas	Reaguoti į anomaliją
Aprašymas	Administratorius reaguoja į anomaliją (nuokrypis nuo normos).
Aktoriai	Administratorius
Pradinės sąlygos	Administratorius turi prisijungti prie sistemos.
Pagrindiniai žingsniai	Administratorius prisijungia prie sistemos ir reaguoja į anomaliją
Išskirtinės situacijos	Sistema neveikia. Nėra anomalijų.
Galutinės sąlygos	Administratorius reaguoja į anomaliją.



2.14 pav. Sistemos panaudos atvejo diagrama

Įvykių duomenų įrašymas į duomenų bazę panaudos atvejo aprašymas pateiktas 2.10 lentelėje. Sistema gautus duomenis apie įvykius iš serverių ar virtualių mašinų, kuriose įdiegtas OOSEC agentas, įrašo į duomenų bazę.

2.10 lentelė Įvykių duomenų įrašymas į duomenų bazę panaudos atvejo aprašymo lentelė

ID	PA-01
Pavadinimas	Įrašo įvykių duomenis į duomenų bazę
Aprašymas	Sistema gaunamus įvykių duomenis iš serverių, virtualių mašinų įrašinėja į duomenų bazę.
Aktoriai	Sistema
Pradinės sąlygos	Pridedami įrenginiai į OSSIM aplinką.
Pagrindiniai žingsniai	Sistema turi tinkamai veikti. Įrenginiai turi siųsti įvykių duomenis.
Išskirtinės situacijos	Sistema neveikia.
Galutinės sąlygos	Įvykių duomenys įrašomi į duomenų bazę.

Žurnalinių įrašų rinkimo panaudos atvejo aprašymas pateiktas 2.11 lentelėje. Sistema renka žurnalinius įrašus iš serverių ar virtualių mašinų, kuriose įdiegtas OSSEC agentas.

2.11 lentelė Žurnalinių įrašų rinkimo panaudos atvejo aprašymo lentelė

ID	PA-02
Pavadinimas	Rinkti žurnalinius įrašus
Aprašymas	Sistema gauna ir renka žurnalinius įrašus iš serverių virtualių mašinų, kuriose yra įdiegti OSSEC agentai.
Aktoriai	Sistema
Pradinės sąlygos	Virtualiose mašinose, serveriuose įdiegiami OSSEC agentai.
Pagrindiniai žingsniai	Sistema turi tinkamai veikti. Gauna žurnalinius įrašus iš virtualių mašinų, serverių.
Išskirtinės situacijos	Sistema neveikia. Nėra įdiegtų OSSEC agentų.
Galutinės sąlygos	Sistema renka žurnalinius įrašus.

Žurnalinių analizės panaudos atvejo aprašymas pateiktas 2.12 lentelėje. Sistema analizuoja žurnalus iš serverių ar virtualių mašinų, kuriose įdiegtas OSSEC agentas pagal aprašytas centralizuotas ar globalias taisykles.

2.12 lentelė Žurnalinių analizės panaudos atvejo aprašymo lentelė

ID	PA-03
Pavadinimas	Žurnalų analizė
Aprašymas	Sistema žurnalinius įrašus analizuoja pagal aprašytas centralizuotas ar globalias taisykles.
Aktoriai	Sistema
Pradinės sąlygos	Virtualiose mašinose, serveriuose įdiegiami OSSEC agentai.
Pagrindiniai žingsniai	Sistema turi tinkamai veikti. Gauna žurnalinius įrašus iš virtualių mašinų, serverių ir analizuoja pagal centralizuotas ar globalias taisykles.
Išskirtinės situacijos	Sistema neveikia. Nėra įdiegtų OSSEC agentų.
Galutinės sąlygos	Sistema renka žurnalinius įrašus ir analizuoja pagal aprašytas globalias ar centralizuotas taisykles.

Įvykių normalizavimo panaudos atvejo aprašymas pateiktas 2.13 lentelėje. Sistema gautus įvykius iš virtualios mašinos, kurioje yra įdiegtas OSSEC agentas, normalizuoja įvykius OSSEC serveriui suprantama struktūra.

2.13 lentelė Įvykių normalizavimo panaudos atvejo aprašymo lentelė

ID	PA-04
Pavadinimas	Įvykių normalizavimas
Aprašymas	Sistema įvykius normalizuoja serveriui suprantama struktūra
Aktoriai	Sistema
Pradinės sąlygos	Virtualiose mašinose, serveriuose įdiegiami OSSEC agentai.
Pagrindiniai žingsniai	Sistema turi tinkamai veikti ir OSSEC agentas turi būti paleistas kliento virtualioje mašinoje.
Išskirtinės situacijos	Sistema neveikia. Nėra įdiegtų OSSEC agentų.
Galutinės sąlygos	Sistema normalizuoja gautus įvykius iš kliento virtualios mašinos ir siunčia OSSEC serveriui suprantama struktūra.

2.2. Nefunkciniai reikalavimai

„Incidentų kompiuterių tinkluose identifikavimas, taikant anomalijų aptikimo metodus“ nefunkciniai reikalavimai:

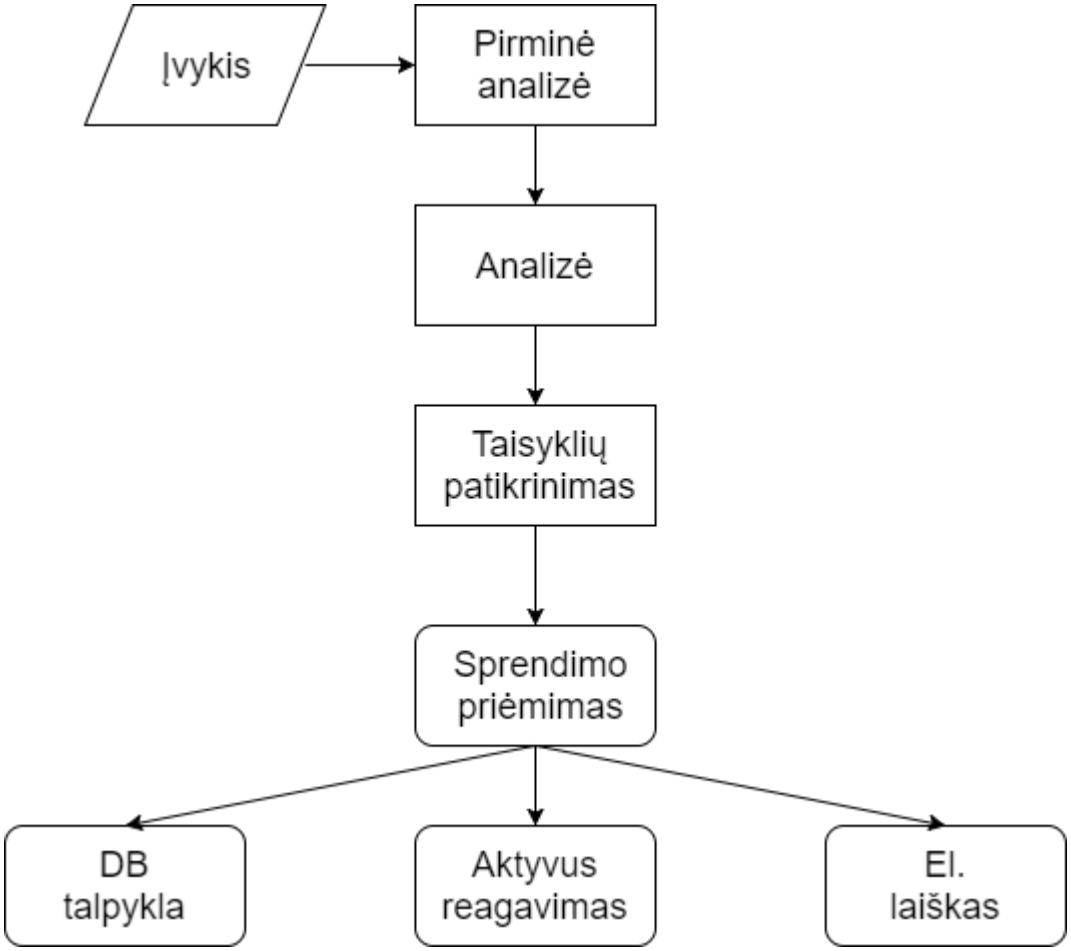
- OSSIM jutiklis – OSSEC agentas, įsibrovimo aptikimo sistema „Snort“;
- operacinė sistema – OSSEC agentai turi būti įdiegti į Linux ir Windows operacines sistemas;
- valdymo įrankis – OSSIM.

„Incidentų kompiuterių tinkluose identifikavimas, taikant anomalijų aptikimo metodus“ nefunkciniai reikalavimai, OSSEC agento diegimo:

- OSSEC agento atsiuntimas – agentas turi būti siunčiamas iš oficialios internetinės svetainės, kurioje patalpinta OSSEC agento sisteminiai failai;
- OSSEC agento diegimas – agentas turi būti diegiamas pagal nurodytus diegimo žingsnius oficialioje internetinėje svetainėje, kurioje patalpinta OSSEC agento sisteminiai failai;
- OSSEC agento konfigūravimas – agento konfigūravimas turi būti atliekamas pagal nurodytus konfigūravimo žingsnius oficialioje internetinėje svetainėje, kurioje patalpinta OSSEC agento sisteminiai failai;
- OSSEC agento paleidimas – paleidimas turi būti atliekamas pagal nurodytus paleidimo žingsnius oficialioje internetinėje svetainėje, kurioje patalpinta OSSEC agento sisteminiai failai.

2.3. Įvykio analizės procesas

2.15 pav. pateikta įvykio diagrama, kaip OSSEC apdoroja įvykį.



2.15 pav. Įvykio apdorojimo diagrama [18]

Kai tik įvykis yra gaunamas, OSSEC bando iššifruoti ir ištraukti bet kokią tinkamą informaciją iš jo. Iššifravimas ar įvykio normalizavimas yra išskaidytas į dvi dalis: pirminę analizę ir analizę.

2.14 lentelėje pateikiami atrinkti laukai po įvykio analizės [18].

2.14 lentelė Įvykio atrinkti laukai

Laukas	**Aprašymas**
Log	Įvykio žinutės skyrius
Full_log	Visas įvykis
location	Iš kur atėjo žurnalas
hostname	Įvykio šaltinio kompiuterio vardas
Program_name	Programos vardas. Paimama iš „syslog“ įvykio antraštės
scrip	Šaltinio IP adresas įvykio viduje
dstip	Paskirties IP adresas įvykio viduje
srcport	Šaltinio prievadas įvykio viduje
dstport	Paskirties prievadas įvykio viduje
protocol	Protokolas įvykio viduje
action	Veiksmas paimtas iš įvykio vidaus
srcuser	Šaltinio vartotojo vardas
dstuser	Paskirties vartotojo vardas
id	Identifikacijos numeris iš įvykio
status	Iššifruotas statusas įvykio viduje
id	Identifikacijos numeris
command	Kviesta komanda įvykio viduje
url	Internetinis adresas įvykio viduje
data	Data
systemname	Sistemos vardas įvykio viduje

1. Įvykio pirminė analizė – pirminės analizės procesas yra skirtas, kad ištrauktų tik statišką informaciją iš žinomų įvykio laukų. Informacija ištraukta per šią fazę yra laikas, data, kompiuterio vardas, programos pavadinimas ir žurnalinė žinutė.

2. Įvykio analizė – tai kitas žingsnis procese, po pirminės analizės. Analizės tikslas ištraukti nestatišką informaciją iš įvykių. Iš gautos informacijos, vėliau galime panaudoti mūsų aprašomas taisykles. Aprašytomis taisyklėmis galime išgauti IP adreso informaciją, vartotojo vardus ir kitus panašius duomenis.

3. Taisyklės – OSSEC turi dviejų tipų taisykles: atomines (angl. *atomic*) ir sudėtines (angl. *composite*). Atominės taisyklės yra pagrįstos tik vienetiniams įvykiams, be jokios koreliacijos. Sudėtinės taisyklės pagrįstos pasikartojančiais įvykiais.

4. Sprendimo priėmimas – duomenys įrašomi į duomenų bazę. Siunčiami el. laiškai, sistemos administratoriui. Aktyvus reagavimas – IP adreso blokavimas, vartotojo įspėjimas apie žalingą veiklą.

2.4. Taisyklių rašymas

Kiekviena OSSEC taisyklė patalpinta katalogo viduje *rules/*. Dažniausiai patalpinta */var/ossec/rules/*. Kiekviena taisyklė yra apibrėžta atskiroje XML rinkmenoje. Numatytas standartinis OSSEC agento įdiegimas savyje turi 56 taisyklių rinkmenas.

Kiekviena taisyklė turi unikalų identifikacijos numerį nuo 0 iki 99,999. Vartotojui palikta nuo 100,000 iki 109,999.

OSSEC sunkumo (angl. *severities*) lygmuo svyruoja nuo 0 iki 15, 0 žemiausias 15 aukščiausias. Kai taisyklės parašytos, jos yra suskirstytos naudojant hierarchinį modelį, kuo aukštesnis sunkumo lygmuo, tuo įvykiai yra tikrinami pirmiau. Vienintelė išimtis – jei sunkumo lygmuo yra 0, tai šis vertinamas prieš visus kitus sunkumo lygmenis.

Taisyklės yra aprašomos serverio pusėje, pagal kurias stebimoje sistemoje renkami įvykiai.

Kliento pusėje, virtualioje mašinoje su „Linux“ operacine sistema parašyta taisyklė, kuri realiu laiku stebi pasirinktą svarbią direktoriją, šiuo atveju */var/www/html* direktorija:

```
<directories realtime="yes" report_changes="yes" check_sum="yes">/var/www/html</directories>
```

Pasirinktas „*realtime*“ atributas, kuris reiškia, jog realiu laiku stebės pasikeitimus šioje direktorijoje. Atributu „*report_changes*“ nurodoma, jog generuotų įspėjimus apie šioje direktorijoje įvykusius pasikeitimus. „*check_sum*“ atributas nurodomas tuo atveju, jei norima stebėti failų vientisumo pasikeitimus. Šia taisykle norima identifikuoti visus pasikeitimus šioje direktorijoje, kurie atliekami be administratoriaus žinios. Dažniausiai, kai į tinklalapį yra įsilaužiama, programišius prideda kenkėjiškų bylų, kurios atlieka žalingą veiklą. Taip pat dažnas atvejis, kai programišius palieka atgalinį įėjimą (angl. *backdoor*). Taigi šios taisyklės pagrindinis darbas realiu laiku pastebėti bet kokius pasikeitimus šioje direktorijoje ir siųsti pranešimą į OSSEC serverį.

Kliento pusėje, virtualioje mašinoje su „Windows“ operacine sistema parašyta taisyklė, kuri siunčia įvykius apie „Windows powershell“ aktyvumą, taisyklės aprašymas:

```
<logall>yes</logall>
<localfile>
   <location>Windows PowerShell</location>
   <log_format>eventlog</log_format>
</localfile>
```

„<localfile> </localfile>“ viduje aprašoma, iš kur bus skaitomi žurnaliniai įrašai ir kokiu formatu bus skaitoma. Šiuo atveju vieta, iš kur imami žurnaliniai įvykiai yra „Windows PowerShell“, o žurnalinių įvykių formatas yra „eventlog“. „eventlog“ formato nurodymas naudojamas „Windows“ operacinėje sistemoje. Šios taisyklės pagrindinis darbas identifikuoti ir pranešti į OSSEC serverį apie „Windows Powershell“ aktyvumą. Serverio pusėje aprašytos taisyklės virtualiai mašinai su „Linux“ operacine sistema, pagal kurias aptinkama anomalija, naujų failų atsiradimo stebėjimas:

```
<rule id="554" level="7" overwrite="yes">
   <category>ossec</category>
   <decoded_as>syscheck_new_entry</decoded_as>
   <match>/var/www/html</match>
   <description>File added to the /var/www/html directory </description>
   <group>syscheck</group>
 </rule>
```

Nurodomas taisyklės identifikacijos numeris „554“, nustatomas sunkumo lygis „7“, kuris nurodo taisyklės svarbumą, taip pat nurodome, jog perrašome esamą taisyklę. Pasirenkame kategoriją „ossec“.

Nurodome, ko ieškome sistemos patikrinimo metu, šiuo atveju naujų pridėtų failų. Toliau nurodome, kurioje direktorijoje stebimas naujų failų atsiradimas. Aprašome, kaip pranešimas bus spausdinamas bei nurodome grupę „syscheck“, o šio patikrinimo metu bus ieškomas šis aprašytas incidentas.

Serverio pusėje aprašytos taisyklės virtualiai mašinai su „Linux“ operacine sistema, pagal kurias aptinkama anomalija, failų pasikeitimo stebėjimas:

```
<rule id="550" level="15" overwrite="yes">
  <category>ossec</category>
  <decoded_as>syscheck_integrity_changed</decoded_as>
  <match>/var/www/html</match>
  <description>File in /var/www/html directory has been modified!</description>
  <group>syscheck,</group>
</rule>
```

Nurodomas taisyklės identifikacijos numeris „550“, nustatomas sunkumo lygis „15“, kuris nurodo taisyklės svarbumą, taip pat nurodome, jog perrašome esamą taisyklę. Pasirenkame kategoriją „ossec“. Nurodome, ko sistemos patikrinimo metu ieškoma, šiuo atveju tai failo pasikeitimo stebėjimas. Toliau nurodome, kurioje direktorijoje stebimas failų pasikeitimas. Aprašome, kaip pranešimas bus spausdinamas bei nurodome grupę „syscheck“, o šio patikrinimo metu bus ieškomas šis incidentas aprašytas taisykle.

Serverio pusėje aprašytos taisyklės virtualiai mašinai su „Windows“ operacine sistema, pagal kurias aptinkama „Windows PowerShell“ veikla:

```
<group name="powershell,">
  <rule id="100210" level="15">
    <if_sid>18100,18101</if_sid>
    <match>CommandType=Script</match>
    <description>Powershell Script.</description>
  </rule>
  <rule id="100211" level="15">
    <if_sid>18100,18101</if_sid>
    <match>CommandType=Cmdlet</match>
    <description>Powershell Command.</description>
  </rule>
  <rule id="100212" level="15">
    <if_sid>18100,18101</if_sid>
    <match>CommandType=Function</match>
    <description>Powershell Function.</description>
  </rule>
 <rule id="100219" level="15">
    <if_sid>18100,18101</if_sid>
    <match>CommandType=Application</match>
    <description>Powershell Command started.</description>
```

```
 </rule>
</group>
```

Šios aprašytos taisyklės tikslas yra pastebėti bet kokią veiklą susijusią su „Windows PowerShell“. Tam, kad ši taisyklė veiktų, reikia atlikti kitus papildomus žingsnius. Sukuriamas failas *powershell.cfg* direktorijoje */var/ossim/agent/plugins* , o tame faile aprašome taisyklę, pagal kurią atliekamas įvykio normalizavimas:

```
[100219 - PowerShell Command Started (500)]
event_type=event
#precheck="INFORMATION"
regexp="^AV\s+\-\sAlert\s+\-\s\"(?P<date>\d+)\"\s\-\-
>\sRID\:\s\"(?P<rule_id>\d+)\"\;\s+RL\:\s+\"(?P<rule_level>\d+)\"\;\s+RG\:\s+\"(?P<rule_group>[^\"
]*)\"\;\s+RC\:\s+\"(?P<rule_comment>[^\"]*)\";.*?HOSTNAME\:[^\)]*\)\s(?P<winip>\S+)-
>.*?INFORMATION\((?P<winevent_id>\d+)\)\:.*NewCommandState=(?P<cmd_
state>[^=]*) SequenceNumber=(?P<seq_num>[^=]*) HostName.*CommandName=(?P<cmd_name>[^=]*)
CommandType=(?P<cmd_type>[^=]*) ScriptName=(?P<script_na
me>[^=]*) CommandPath=(?P<cmd_path>[^=]*) CommandLine=(?P<cmd_line>[^=]*)\[END\]\"\;"
date={normalize_date($date)}
plugin_id={translate($rule_id)}
plugin_sid={$rule_id}
device={resolv($winip)}
src_ip={resolv($winip)}
dst_ip={resolv($winip)}
userdata1={$rule_level}
userdata2={$winevent_id}
userdata3={$cmd_state}
userdata4={$seq_num}
userdata5={$cmd_name}
userdata6={$cmd_type}
userdata7={$script_name}
userdata8={$cmd_path}
userdata9={$cmd_line}
```

Toliau reikia atnaujinti duomenų bazę, sukuriamas failas *powershell.sql* direktorijoje */var/ossim/agent/plugins* ir aprašomi duomenų bazės atnaujinimo veiksmai:

```
DELETE FROM plugin WHERE id=9002;
DELETE FROM plugin_sid WHERE plugin_id=9002;
INSERT INTO plugin (id, TYPE, name, description) VALUES (9002, 1, 'powershell', 'Powershell Script/Function/Command Events');
INSERT INTO plugin_sid (plugin_id, sid, category_id, class_id, name, priority, reliability) VALUES (9002, 100219, NULL, NULL, 'powershell: PowerShell Command Started', 3, 2);
```

Aprašius taisyklę turime paleisti komandą „cat /etc/ossim/agent/plugins/powershell.sql | ossim-db“, kuri atnaujina duomenų bazę ir įrašo naują taisyklę.

Visa tai atlikus reikia perkonfigūruoti OSSIM serverį ir iš naujo paleisti OSSEC agentą.

2.5. Projektinės dalies išvados

Kuriamoje sistemoje yra du aktoriai: administratorius ir sistema. Administratorius naudojasi kuriama sistema tam, kad lengviau identifikuotų incidentą ar anomaliją. Taip pat gali stebėti tinkle esančius įrenginius, realaus laiko tinklo įrenginių saugumo pažeidimo įvykius, atlikti naujo vartotojo pridėjimą prie kuriamos sistemos arba įdiegti OSSEC agentą į virtualias mašinas ar serverius. Sistemos paskirtis – tai įvykių rinkimas iš įvairių nurodytų šaltinių, jų normalizavimas, analizavimas ir įrašymas į duomenų bazę. Kiekvienam aktoriui pateiktos panaudos atvejų diagramos ir jų aprašymo lentelės. Aprašyti funkciniai ir nefunkciniai reikalavimai kuriamai sistemai. Pateikta lentelė kokie duomenys gaunami po įvykių pirminės ir pagrindinės analizės. Aprašyti OSSEC taisyklių sunkumo lygmenys ir rašymo struktūra bei pateiktas taisyklių rašymo pavyzdys.

Sistema pilnai funkcionuoja. OSSEC agentas įdiegtas tiek į „Linux“ operacinę sistemą, tiek į „Windows“, aprašytas detalus veikimas bei pagrindinės galimybės. Taip pat įdiegtos „Snort“ taisyklės, kurios stebi tinklo komponentų srautus.

Aprašytomis naujomis taisyklėmis „Linux“ operacinėje sistemoje OSSEC agentas geba realiu laiku, nustatytose direktorijose pastebėti normalią / nenormalią veiklą. Taip pat aprašytos naujos taisyklės, kurios leidžia stebėti „Windows“ operacinėje sistemoje bet kokią veiklą susijusią su „Windows PowerShell“. Darau išvadą, jog su naujomis aprašytomis taisyklėmis sistema geba daugiau identifikuoti / pastebėti, nei su standartinėmis aprašytomis taisyklėmis.

3. INCIDENTŲ KOMPIUTERIŲ TINKLUOSE IDENTIFIKAVIMAS, TAIKANT ANOMALIJŲ APTIKIMO METODUS TYRIMAS

Atlikus analizę ir projektinę dalį šiame skyriuje pateikiamas projekto tyrimas. Projektas realizuotas pasinaudojus atviro kodo OSSIM valdymo įranku, įdiegtomis „Snort“ taisyklėmis, kurios stebi tinklo srautus. Įdiegti OSSEC agentai į virtualias mašinas, susietas su OSSIM valdymo įrankiu.

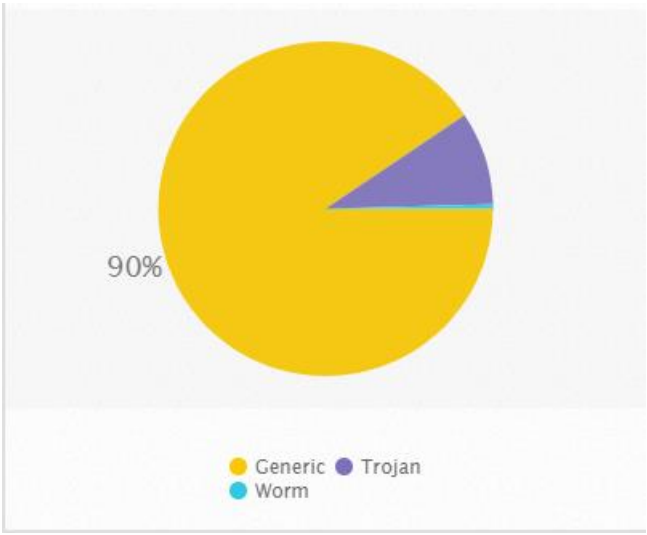
Šio tyrimo tikslas patikrinti ar aprašytos taisyklės geba identifikuoti ir pranešti sistemos administratoriui apie įtartiną, nelegalią veiklą stebimoje sistemoje.

Tyrimo metu tikrinama / tiriama sistemoje aprašytų taisyklių naudingumas, veikimas, informatyvumas, aptikimas:

- ar aprašytos taisyklės geba identifikuoti žalingą / kenkėjišką veiklą;
- ar aprašytos taisyklės geba laiku pastebėti įtartiną veiklą;
- kokias anomalijas, incidentus identifikuoja;
- koks saugos įvykių pažeidimų intensyvumas;
- nereikšmingos informacijos gavimas.

3.1. Projekto tyrimas

Šiame skyriuje pateikiami atlikto tyrimo rezultatai. Duomenys užfiksuoti nuo įvykių įrašinėjimo pradžios iki 2017 m. gegužės 11 d. Tyrimui atlikti naudojami KTU tinkle stebimi įrenginiai.



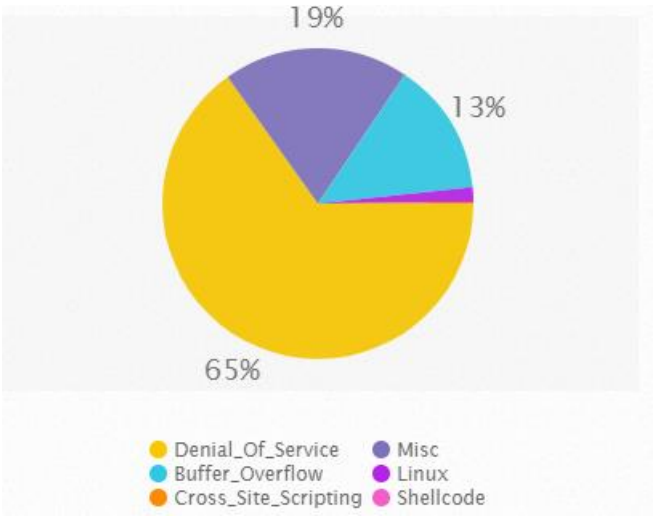
3.1 pav. Kenksmingo kodo įvykių tipai

3.1 pav. pateikti gauti rezultatai, kokie įvykių tipai buvo aptikti sistemos atlikto tyrimo metu. Didžiausią dalį užima bendri įvykių tipai, kurie yra informacinio pobūdžio, toliau matome, jog identifikuotas kenksmingas kodas (angl. *Trojan*) ir kirminas (angl. *worm*). 3.1 lentelėje pateikiamas užfiksuotas įvykių kiekis.

Kenksmingo kodo aptikimo rezultatai parodo, jog sistema geba identifikuoti žalingą veiklą stebimoje sistemoje. Šie duomenys gauti iš tinklo įsibrovimo aptikimo sistemos „Snort“.

3.1 lentelė Užfiksuotas įvykių kiekis

Pavadinimas	**Kiekis**
Bendri (angl. *generic*)	1439
Kenksmingas kodas (angl. *trojan*)	143
Kenksmingas kodas (angl. *worm*)	7



3.2 pav. Pažeidžiamumą išnaudojantys įvykių tipai

3.2 pav. pateikti užfiksuoti pažeidžiamumą išnaudojančių (angl. *Exploit)* įvykių tipai, kokie buvo aptikti daugiausiai kartų. Didžiausią dalį užima bandymai sutrikdyti paslaugą, įvykių tipas. Toliau seka, įvairūs įvykių tipai. Bandymai išnaudoti duomenų perpildymo klaidą (angl. *Buffer_overflow*). 3.2 lentelėje pateikiama pažeidžiamumą išnaudojantys įvykių kiekis.

Pažeidžiamumą išnaudojančių įvykių aptikimo rezultatai parodo, jog sistema geba identifikuoti žinomus pažeidžiamumus stebimoje sistemoje. Šie duomenys gauti iš tinklo įsibrovimo aptikimo sistemos „Snort“.

3.2 lentelė Pažeidžiamumus išnaudojantys įvykių kiekis

Pavadinimas	**Kiekis**
Paslaugos blokavimas (angl. *Denial Of Service*)	2262
Įvairūs įvykių tipai (angl. *misc*)	670
Duomenų perpildymo klaida	481
Linux – bandyta gauti administratoriaus teises	53
Bandymas išnaudoti saityno pažeidžiamumus (angl. *Cross site scripting*)	5
Bandymas išnaudoti programinės įrangos pažeidžiamumus (angl. *Shellcode*)	1

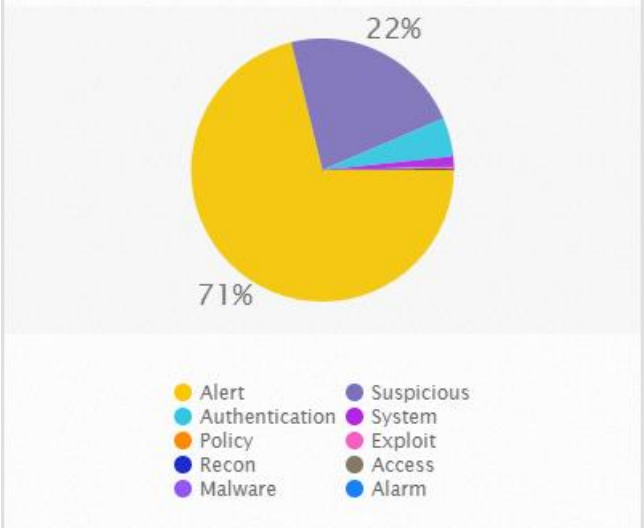
3.3 pav. sėkmingi prisijungimai prie sistemų prieš nesėkmingus prisijungimus

3.3 pav. pateikta sėkmingo ir nesėkmingo prisijungimo atlikto tyrimo duomenys. Didžiausią dalį užima nesėkmingi prisijungimai, tai reiškia, jog aptiktas didelis kiekis bandymų atspėti sistemų prisijungimo duomenis. Sėkmingų prisijungimų pateikti duomenys paveiksle nepasako, jog tiek kartų įsilaužėliui pavyko prisijungti prie sistemos, į šiuos duomenis įeina ir teisėti prisijungimai. Pagal pateiktus tyrimo duomenis sėkmingi prisijungimai parodyti šiame paveiksle yra teisėti. 3.3 lentelėje pateikta sėkmingų ir nesėkmingų prisijungimų kiekis.

Sėkmingų ir nesėkmingų prisijungimų identifikavimas veikia tinkamai. Iš šios informacijos galime daryti išvadą, jog nuolatos ir intensyviai bandoma patekti į sistemą, bandant atspėti prisijungimo duomenis.

3.3 lentelė Sėkmingų prisijungimų ir nesėkmingų prisijungimų kiekis

Pavadinimas	**Kiekis**
Nesėkmingi prisijungimai	187290
Sėkmingi prisijungimai	41979

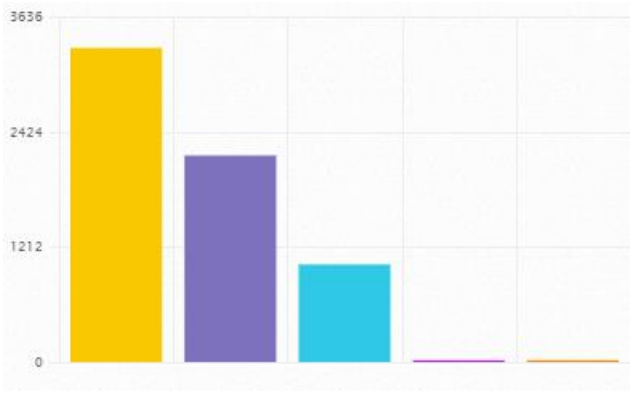


3.4 pav. Dešimt dažniausių aptiktų įvykių tipai

3.4 pav. pateikti atlikto tyrimo metu dešimt dažniausiai pasikartojančių įvykių kategorijos. Didžiausią dalį užima įspėjimai, toliau pagal didžiausią apimtį seka įtariami įvykiai, bandymai prisijungti ir sistemos. 3.4 lentelėje pateikta aptiktų įvykių kiekis.

3.4 lentelė Aptiktų įvykių kiekis

Pavadinimas	**Kiekis**
Įspėjimas (angl. *alert*)	1069375
Įtartini (angl. *suspicious*)	336241
Tapatybės nustatymas (angl. *authentication*)	71087
Sistema (angl. *system*)	18666
Taisyklės (angl. *policy*)	1996
Žinomų pažeidžiamumų išnaudojimas (angl. *exploit*)	1701
Mėginimai išgauti naudingą informaciją (angl. *recon*)	1676
Prieiga (angl. *access*)	639
Kenkimo programa (angl. *malware*)	227
Pavojaus signalas (angl. *alarm*)	192

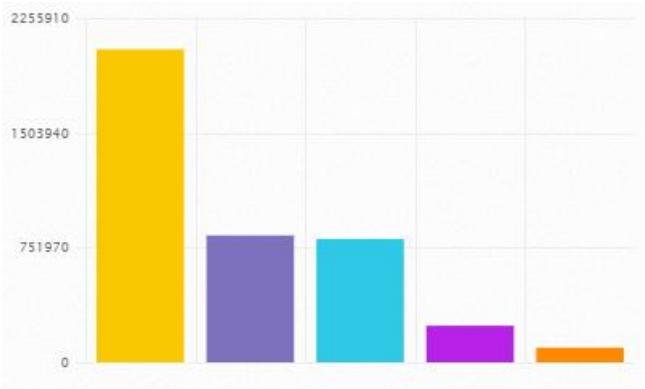


3.5 pav. Saugumo įvykiai: aptikti penki pavojaus signalai

3.5 pav. pateikti saugumo įvykiai, penki didžiausi pavojaus signalai (angl. *alarms*). Didžiausią dalį užima bandymai prisijungti prie OSSIM (angl. *login authentication*) metodu, toliau bandymai prisijungti prie OSSIM (angl. *SSH authentication*) metodu, toliau bandymai prisijungti prie OSSIM (angl. *SSH service authentication*) metodu. 3.5 lentelėje pateikta aptiktų penkių pavojaus signalų kiekis.

3.5 lentelė Saugumo įvykiai: aptiktų penkių pavojaus signalų kiekis

Pavadinimas	**Kiekis**
Bandymai prisijungti prie OSSIM (angl. *login authentication*) metodu	3305
Bandymai prisijungti prie OSSIM (angl. *SSH authentication*) metodu	2173
Bandymai prisijungti prie OSSIM (angl. *SSH service authentication*) metodu	1026
Bandymai prisijungti prie Windows (angl. *windows authentication*) metodu	19
Aptiktos P2P paslaugos	19

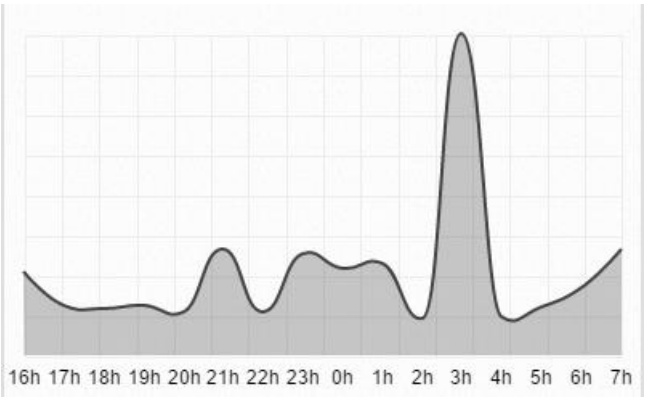


3.6 pav. Saugumo įvykiai: aptikti penki įvykiai

3.6 pav. pateikti atrinkti penki dažniausi įvykiai. Didžiausią dalį užima mažos rizikos įsibrovimo aptikimo sistemos įvykiai, toliau seka nežinomas / nepatikimas tinklo srautas, aptikti nestandartiniai protokolai ir potencialiai blogas tinklo srautas. 3.6 lentelėje pateikiamas aptiktų penkių dažniausiai pasikartojančių įvykių kiekis.

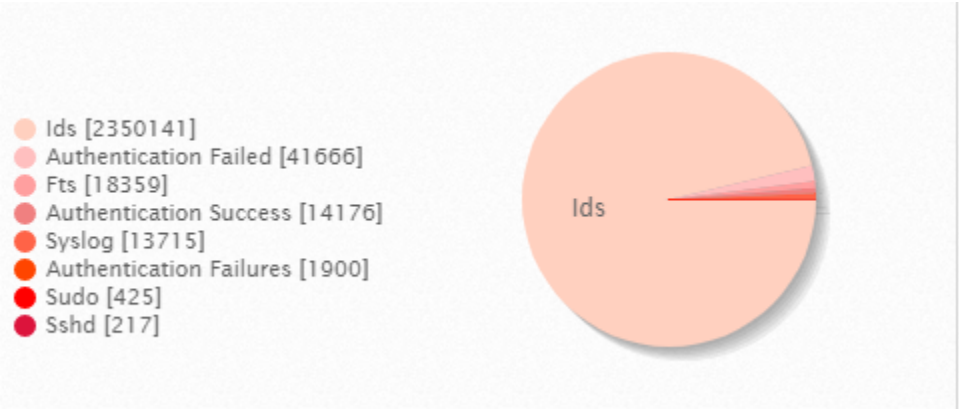
3.6 lentelė Saugumo įvykiai: aptiktų įvykių kiekis

Pavadinimas	**Kiekis**
Įsibrovimo aptikimo sistemos įvykiai	2050827
Nežinomas / nepatikimas tinklo srautas.	831466
Aptikti nestandartiniai protokolai	808303
Potencialiai blogas tinklo srautas	240094
Prieš saityną ataka arba skenavimas	95950



3.7 pav. Įvykių intensyvumas valandos intervalu

3.7 pav. pateiktas saugumo įvykių intensyvumo fiksavimas valandos intervalu. Pastebėta, jog apie 3 val. nakties buvo užfiksuota didžiausias įvykių kiekis, iš viso 239427 įvykių. Kitu laiku nuo 35000 iki 75000 įvykių.



3.8 pav. OSSEC agento įvykių aptikimo duomenys

3.8 pav. pateikta atlikto tyrimo rezultatų duomenys. Atrinkti aštuoni didžiausi užfiksuoti įvykiai. Iš šių duomenų matome jog didžiausią dalį užima įvykiai kurie pateikti, kaip „Ids“. Aptikti nesėkmingi prisijungimai, iš šių duomenų galime teigti, jog nuolat bandoma patekti į sistemą spėliojant prisijungimo duomenis. Išrikiuoti ir sėkmingų prisijungimų duomenys, atlikus sėkmingų prisijungimų tyrimą, neidentifikuota neteisėtų prisijungimų.

Tarp šių duomenų identifikuotų, kaip „Ids“, taip pat yra naujai aprašytų taisyklių, kurios virtualioje mašinoje su „Linux“ operacine sistema seka realiu laiku paskirtoje direktorijoje failų pasikeitimus ir naujų failų pridėjimo įvykius. Tačiau dėl mažiau reikšmingos kitos gausios informacijos, užgožiami įvykiai su naujai sukurtomis / perrašytomis taisyklėmis. Taip pat į šiuos duomenis įeina ir aprašytos taisyklės, kurios virtualioje mašinoje su operacine sistema „Windows“ stebi „Windows PowerShell“ aktyvumą realiu laiku. Bet ir šie duomenys taip pat nepatenka į šią pateiktą duomenų diagramą.

Pagal panašių sistemų tyrimo rezultatus, kitos sistemos taip pat identifikuoja sėkmingus ir nesėkmingus prisijungimo duomenis. Aptinka kenksmingą kodą, žinomus pažeidžiamumus bei realiu laiku stebi failų pasikeitimus [19] [20] [21]. Tačiau nerasta informacijos, jog kuri nors sistema stebėtų „Windows PowerShell“ aktyvumą.

Šiuo tyrimu norima parodyti, jog sistema kuri yra atviro kodo, galima išnaudoti ją produktyviai ir gauti panašius duomenis, kaip ir sistemos kurios prašo atlygio už jų teikiamas paslaugas. Taisyklių aprašymas yra nesudėtingas, galima lengvai apsirašyti norimas taisykles ir pagal jas ieškoti pažeidžiamumų ar stebėti ir identifikuoti kenkėjišką veiklą.

3.2. Projekto tyrimo apibendrinimas

Pagal tyrimo rezultatus matome, jog kuriama sistema pilnai geba identifikuoti ir generuoti įvykius, pagal nustatytas OSSEC ir „Snort“ taisykles. Pateikti KTU tinklo stebimų įrenginių tyrimo rezultatai yra nepilni, kiti duomenys yra viešai neskelbiami. Pagal tyrimo rezultatus galime teigti, jog sistema geba identifikuoti ir pranešti apie kenksmingą kodą, žinomus pažeidžiamumus, taip pat apie sėkmingus ir nesėkmingus prisijungimus prie sistemos. Taip pat parodoma, jog su jog sistema kuri yra

atviro kodo, galima išnaudoti ją produktyviai ir gauti panašius duomenis, kaip ir sistemos, kurios yra mokamos.

4. REZULATŲ APIBENDRINIMAS IR IŠVADOS

1. Pateikti tinklo anomalijų aptikimo metodai: statistinis, klasifikavimu grįstas, taisyklėmis grįstas, klasterizavimo metodas.
2. Išanalizuota įsibrovimo aptikimo sistema remiantis OSSEC ir „Snort“ pavyzdžiu. Įsibrovimo aptikimo funkcijas apima: stebimi ir analizuojami vartotojo veiksmai, sistema ir tinklo aktyvumas; konfigūruojama sistema, generuojanti ataskaitas apie galimus pažeidžiamumus; vertinama sistema ir failų vientisumas; atpažįstami žinomų atakų modeliai; analizuojama nenormali veikla; vartotojo taisyklių pažeidimų sekimas.
3. Pateiktos ir išanalizuotos panašios sistemos į pasirinktą, tad galime teigti, jog OSSIM geriausiai atitinka iškeltus lyginimo kriterijus. Todėl pasinaudojant OSSIM (Open source Security Information and Event management) platforma yra įdiegiama, realiu laiku veikianti sistema.
4. Šiame darbe patobulinta OSSIM valdymo įrankio efektyvumas, naudingumas, informatyvumas, pastebimumas pasinaudojant OSSEC agento galimybėmis. OSSEC agentu, OSSIM valdymo įrankyje, aprašyti metodas, kurie stebimose sistemose rinka informaciją apie aptiktas anomalijas
5. Kuriamoje sistemoje yra du aktoriai: administratorius ir sistema. Administratorius naudojasi kuriama sistema tam, kad lengviau identifikuotų incidentą ar anomaliją. Taip pat jis gali stebėti tinkle esančius įrenginius, realaus laiko tinklo įrenginių saugumo pažeidimo įvykius, atlikti naujo vartotojo pridėjimą prie kuriamos sistemos arba įdiegti OSSEC agentą į virtualias mašinas ar serverius. Sistemos paskirtis yra įvykių rinkimas iš įvairių nurodytų šaltinių, jų normalizavimas, analizavimas ir įrašymas į duomenų bazę. Kiekvienam aktoriui pateiktos panaudos atvejų diagramos ir jų aprašymo lentelės. Aprašyti funkciniai ir nefunkciniai reikalavimai kuriamai sistemai. Pateikta lentelė, kokie duomenys gaunami po įvykių pirminės ir pagrindinės analizės. Aprašyti OSSEC taisyklių sunkumo lygmenys ir rašymo struktūra.
6. Sistema pilnai funkcionuoja. OSSEC agentas įdiegtas tiek į „Linux“ operacinę sistemą, tiek į „Windows“, aprašytas detalus veikimas bei pagrindinės galimybės. Taip pat įdiegtos „Snort“ taisyklės, kurios stebi tinklo komponentų srautus.
7. Aprašytomis naujomis taisyklėmis „Linux“ operacinėje sistemoje OSSEC agentas geba realiu laiku, nustatytose direktorijose pastebėti normalią / nenormalią veiklą. Taip pat aprašytos naujos taisyklės, kurios leidžia stebėti „Windows“ operacinėje sistemoje bet kokią veiklą susijusią su „Windows PowerShell“. Darau išvadą, jog su naujomis aprašytomis taisyklėmis sistema geba daugiau identifikuoti / pastebėti, nei su standartinėmis aprašytomis taisyklėmis.

8. Pagal tyrimo rezultatus matoma, jog kuriama sistema pilnai geba identifikuoti ir generuoti įvykius, pagal nustatytas OSSEC ir „Snort“ taisykles. Pateikti KTU tinklo stebimų įrenginių tyrimo rezultatai yra nepilni, kiti duomenys yra viešai neskelbiami. Pagal tyrimo rezultatus galime teigti, jog sistema geba identifikuoti ir pranešti apie kenksmingą kodą, žinomus pažeidžiamumus, taip pat apie sėkmingus ir nesėkmingus prisijungimus prie sistemos. Taip pat parodoma, jog su sistema, kuri yra atviro kodo, galima išnaudoti ją produktyviai ir gauti panašius duomenis, kaip ir sistemos, kurios yra mokamos

5. LITERATŪRA

[1] ecsirt.net, „WP4 Clearinghouse Policy - Release 1.2,“ [Tinkle]. Available: http://www.ecsirt.net/cec/service/documents/wp4-clearinghouse-policy-v12.html#HEAD6. [Kreiptasi 05 02 2017].

[2] T. M. T. G. K. S. Paul Cichonski, „Computer Security Incident Handling Guide,“ National Institute of Standards and Technology, U.S., 2012.

[3] Z. K. M. H. K. Rahul Rastogi, „Network Anomalies Detection Using Statistical Technique : A Chi- Square approach,“ *IJCSI International Journal of Computer Science Issues,*, t. 9, nr. 2, pp. 515-522, March 2012.

[4] A. N. M. H. Mohiuddin Ahmed, „A survey of network anomaly detection techniques,“ *Journal of Network and Computer Applications,* pp. 19-31, November 2015.

[5] M. T. a. C. Ji, „Anomaly Detection in IP Networks,“ *IEEE TRANSACTIONS ON SIGNAL PROCESSING*, t. 51, pp. 2191-2204, 2014.

[6] D. K. B. a. J. K. K. Monowar H. Bhuyan, „Network Anomaly Detection: Methods, Systems and Tools,“ *IEEE Communications Surveys & Tutorials,* t. 16, pp. 303-336, March 2014.

[7] A. A. A. H. M. E. Tarek M Mahmoud, „A Hybrid Snort-Negative Selection Network Intrusion Detection Technique,“ *International Journal of Computer Applications,* t. 146, pp. 24-31, July 2016.

[8] R. Underwood, „Impact of Network Security Vulnerabilities Management,“ reseachgate, East Carolina, 2016.

[9] AlienVault, „AlienVault Installation Guide,“ 2010. [Tinkle]. Available: https://scadahacker.com/library/Documents/Manuals/AlienVault_Installation_Guide.pdf. [Kreiptasi 06 02 2017].

[10] R. Kannan, „Journey of Security Incident & Event Management (SIEM)“.

[11] O. R. T. B. Kelly M. Kavanagh, „2016 Magic Quadrant for SIEM,“ 2016. [Tinkle]. Available: https://www.securelink.be/wp-content/uploads/sites/2/2016-Magic-Quadrant-for-SIEM.pdf. [Kreiptasi 07 02 2017].

[12] IBM, „IBM Security QRadar SIEM,“ 2013. [Tinkle]. Available: http://www.draware.dk/files/users/Monica/QRadar_SIEM.pdf. [Kreiptasi 07 02 2017].

[13] IBM, „Getting Started Guide,“ 2016. [Tinkle]. Available: http://public.dhe.ibm.com/software/security/products/qradar/documents/7.2.8/en/b_qradar_gs_guide.pdf. [Kreiptasi 06 02 2017].

[14] S. Enterpirse, „Splunk,“ [Tinkle]. Available: https://www.splunk.com/web_assets/pdfs/secure/Splunk_Product_Datasheet.pdf. [Kreiptasi 07 02 2017].

[15] intellipaat, „Splunk Tutorial,“ [Tinkle]. Available: https://intellipaat.com/tutorial/splunk-tutorial/. [Kreiptasi 06 02 2017].

[16] D. B. Cid, „Log Analysis using OSSEC,“ [Tinkle]. Available: http://ossec.net/ossec-docs/auscert-2007-dcid.pdf. [Kreiptasi 06 02 2017].

[17] manageengine, „manageengine.com,“ [Tinkle]. Available: https://download.manageengine.com/network-monitoring/monitoring-windows-eventlogs.pdf. [Kreiptasi 02 03 2017].

[18] ossec.net, „Working with Rules,“ 2008. [Tinkle]. Available: http://www.ossec.net/ossec-docs/OSSEC-book-ch4.pdf.

[19] I. s. systems, „QRadar SIEM and FireEye MPS Integration,“ [Tinkle]. Available: http://docplayer.net/2407869-Qradar-siem-and-fireeye-mps-integration.html. [Kreiptasi 10 05 2017].

[20] NNT, „SECURE, CENTRALIZED EVENT LOG MANAGEMENT (SIEM),“ [Tinkle]. Available: https://www.newnettechnologies.com/secure-centralized-event-log-management.html. [Kreiptasi 10 05 2017].

[21] SecurityIntelligence, „IBM MaaS360 Enters the Mix on the IBM Security App Exchange,“ [Tinkle]. Available: https://securityintelligence.com/ibm-maas360-enters-the-mix-on-the-ibm-security-app-exchange/. [Kreiptasi 10 05 2017].