VILNIAUS UNIVERSITETAS

INFORMACINIŲ TECHNOLOGIJŲ TAIKYMO CENTRAS

Projektas

09.3.3-ESFA-V-711-01-0003

Mokslo ir studijų institucijoms LITNET teikiamų IT paslaugų plėtra

2.2.1. veikla. Ankstyvo perspėjimo apie grėsmes paslauga

Paslaugos naudojimosi instrukcija

Institucija, norinti pasinaudoti ankstyvo perspėjimo apie grėsmes paslauga, turi užpildyti prašymą (https://www.litnet.lt/lt/vyk-projektai/119-projektai/156-rezultatai-paslaugos#vieningo-prisijungimo-sistemos-sso-paslauga). Paslaugos užsakymui reikia nurodyti sensorių kiekį, atsakingo asmens kontaktus. Taip pat atsiųsti būsimų naudotojų prisijungimo vardus (institucijos SSO ar vietinio prisijungimo, pvz. vu00000, lit000), kontaktinius duomenis ir jiems suteikiamas teises savo institucijoje (administravimas ar tik stebėjimas).

Gautus sensorius reikia sukonfigūruoti pagal sensorių pradinės konfigūracijos instrukcijas ir pastatyti savo tinkle. Ankstyvo perspėjimo apie grėsmes sistemos (toliau APGS) administratoriui reikia nurodyti, kur pastatyti sensoriai pagal jų inventorinį numerį: padalinio sutrumpinimą, norimą sensoriaus pavadinimą ir suteiktą IP adresą. Informacija ir valdymas pasiekimi per naršyklę, adresu https://apgs.litnet.vu.lt (Internet Explorer neveikia). Naudotojai autentifikuojami institucijos vieningo prisijungimo sistemoje (SSO), kuri yra prijungta prie LITNET FEDI. Kadangi sistema prieinama ne visiems naudotojams, prisijungimo duomenys ir jų prieigos teisės prieš tai turi būti suderinti su APGS administratoriumi. Toliau aprašomas paslaugos tinklapio funkcionalumas naudotojams.

1. Pagrindinis meniu

1.1. *Pradžia* – pradinis aplikacijos langas, kuriame yra statistika apie veikiančius sensorius ir įvykius.

1.2. *Žemėlapis* – pasaulio žemėlapis (Pav. 1), kuriame vaizduojami įvykiai pagal šaltinio geografinę poziciją, nurodomi jų tipai ir kiekis. Duomenis galima stebėti realiu laiku arba pasirinkti laikotarpį ir peržiūrėti istoriją, pežiūrėti įvykius iš visų LITNET ar tik dalies sensorių duomenis.

1.3. *Blokavimas* – blokavimo pasirinkimas turi 4 submeniu:

1.3.1. *Taisyklės* – aprašomos taisykles, pagal kurias filtruojami pažeidėjai.

1.3.2. *Pažeidėjai* – sensorių užfiksuotų IP adresų sąrašas ir jų įvykių statistika.

1.3.3. *Baltasis sąrašas* – IP/potinklių sąrašas, kurie nepatenka į pažeidėjų lenteles pritaikius filtrus.

1.3.4. *Potinklių sąrašas* – vietinių IP/potinklių sąrašas, kurių įvykių nematys kitos institucijos, jei jie bus aptikti su sensoriais.

1.4. *Įvykiai* – paskutinių įvykių lentelės pagal sensoriuose veikiančias tarbybas:

1.4.1. *Cowrie* – SSH, Telnet imituojanti tarnyba.

1.4.2. *Dionaea* – HTTP,HTTPS, FTP, TFTP, MSSQL, MySQL paslaugas imituojanti tarnyba.

1.4.3. *Snort* – įsibrovimų aptikimo sistema (IDS).

1.4.4. *Psad* – sisteminių žurnalų tinklo paketų įrašų analizavimo tarnyba.

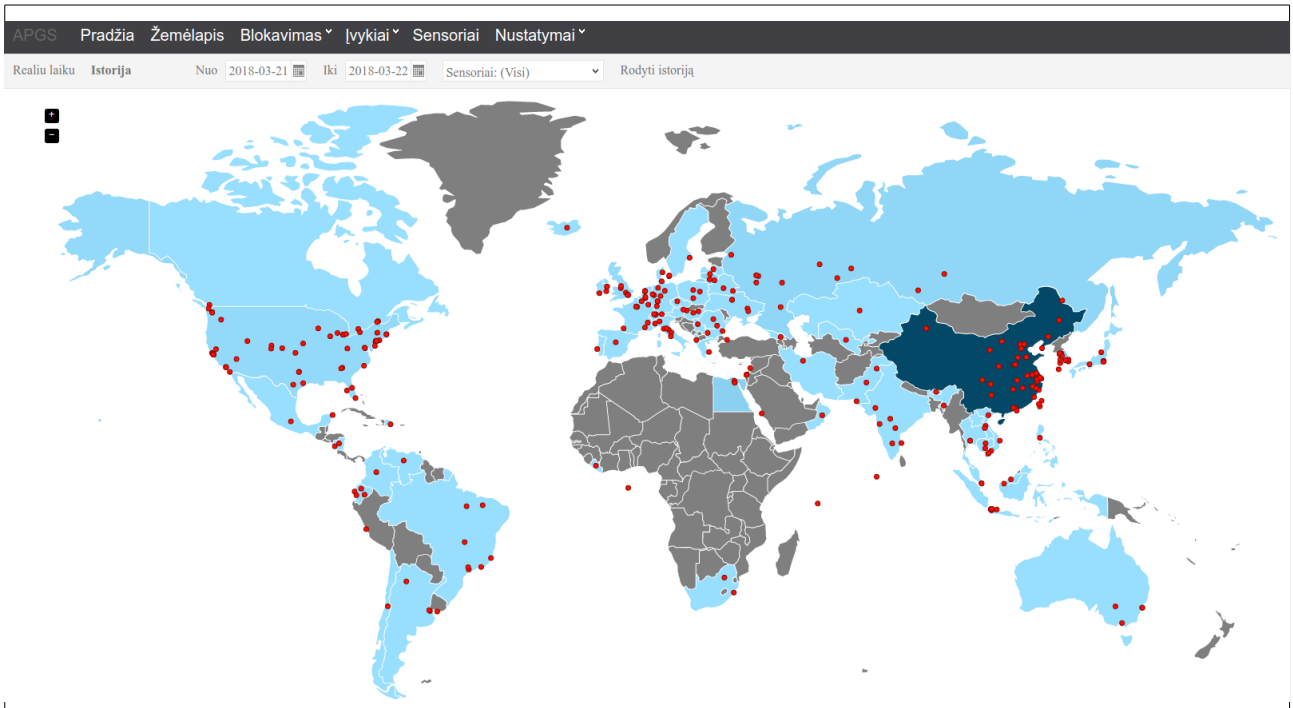
1.5. *Sensoriai* – naudotojo institucijos sensorių sąrašas.

1.6. *Nustatymai* – infromacija apie konfigūravimą, rodomos informacijos nustatymai:

1.6.1. *Instrukcijos* – informacija apie sensorių diegimą, naudojimąsi paslauga.

1.6.2. *Rodomi duomenys* – lentelėse rodomos informacijos pasirinkimas. Galimybė matyti įvykius ir statistiką iš visų sensorių LITNET tinkle ar tik savo institucijos. Numatytasis pasirinkimas yra visi LITNET sensoriai.

1.6.3. *Atsijungti* – išsiregistruoti iš sistemos.



Pav. 1: Įvykių žemėlapis

2. Pažeidėjai ir jų filtravimas

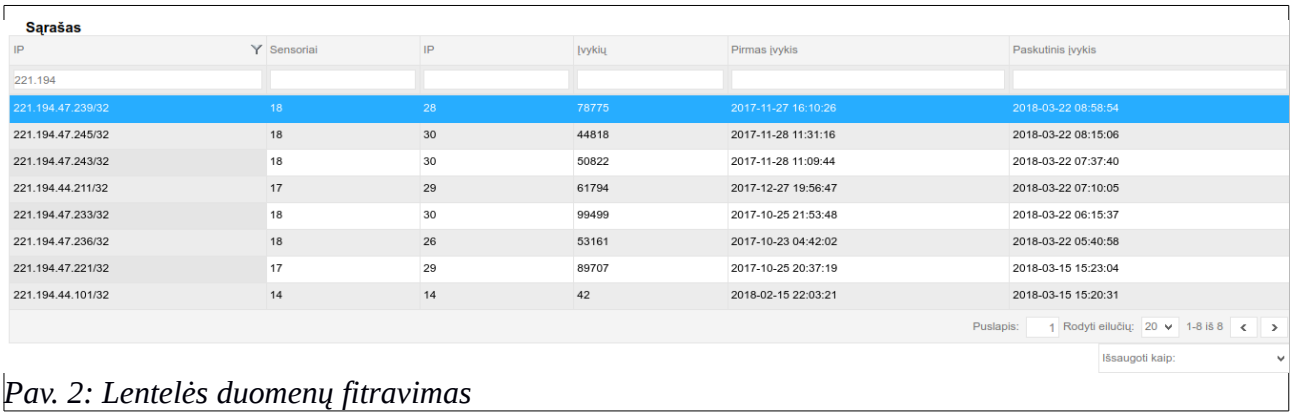
2.1. Pažeidėjų lentelė

Visi sensorių užregistruoti įvykiai yra kaupiami duomenų bazėje. Apie kiekvieną IP adresą renkama statistika:

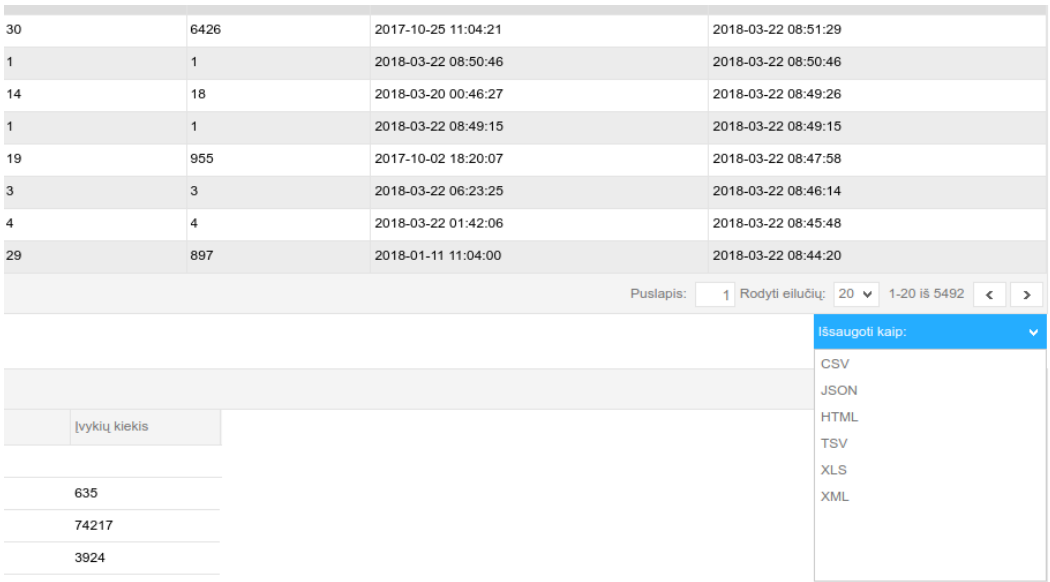
- IP užfiksavę sensoriai, įvykių kiekis;
- Kokie buvo tikslo IP adresai ir įvykių kiekis. Sensoriai gali turėti kelis IP adresus, tai pat gali būti informacijos apie ne į sensorius nukreiptą veiklą (broadcast paketai ir kitas matomas srautas);
- Skirtingi įvykiai ir jų kiekis;
- Pirmo ir paskutinio įvykio data.

Pažeidėjų lentelėje rodomi IP adresai, iš kurių paskutinis įvykis buvo užregistruotas per paskutines 14 parų. Lentelės apačioje yra galimybė išsaugoti lentelės duomenis (Pav. 2) CSV, JSON, HTML, TSV, XLS ir XML formatais. Lentelės duomenys išsaugomi tokie, kokie rodomi naršyklėje, t. y. su pritaikytais viršuje esančiais fitrais (Pav. 3).Paspaudus kairiu pelės mygtuku

ant įrašo žemiau esančioje detalių lentelėje bus parodyta detali informacija apie pažeidėjo paliestus sensorius, sensorių IP, kitų tinklo IP ir įvykius, kiekius.



Pav. 2: Lentelės duomenų fitravimas



Pav. 3: Lentelės duomenų išsaugojimas

2.2. Taisyklės

Ne visi sensorių užfiksuoti įvykiai yra iš kenkėjišką veiklą vykdančių šaltinių, taip pat jei norima pamatyti visus IP vykdančius tam tikras atakas (pvz. 3389/TCP prievado skenavimus) galima sukurti taisykles, pagal kurias bus filtruojami adresai iš pažeidėjų lentelės, jei jie nėra baltąjame sąraše. Pirmiausia sukuriama taisyklių grupė su pagrindiniais parametrais ir vėliau kuriamos tos grupės taisyklės. Dešiniu pelės mygtuku paspaudus ant grupių lentelės (Pav. 4) parodomos 2 galimybės – sukurti naują grupę arba ištrinti esamą (jei buvo paspausta ant egzistuojančios grupės eilutės). Kuriant naują grupę yra 4 parametrai (Pav. 5):

Pavadinimas – grupės pavadinimas (būtina užpildyti).

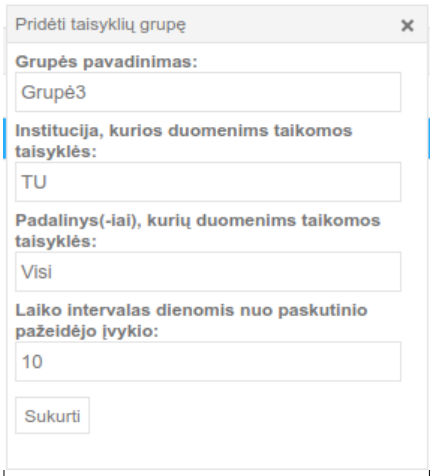
Institucija – institucijos trumpinys, kurios sensorių užfiksuoti įvykiai bus trikrinami. Jei laukelis paliekamas tuščias, bus filtruojami įvykiai iš visų institucijų.

Padaliniai – institucijos padalinys ar padaliniai, rašomi per kablelį, kurių sensorių užfiksuoti įvykiai

bus trikrinami. Jei laukelis paliekamas tuščias, bus filtruojami įvykiai iš visų institucijos padalinių.

Intervalas – laiko intervalas dienomis nuo paskutinio užregistruoto įvykio. Pvz. jei bus įrašytas skaičius 14, tai paskutinis įvykis iš IP adreso turi būti užregistruotas per 2 savaites, kad šis IP būtų rodomas filtrą atitinkančioje lentelėje. Būtina užpildyti.

Pav. 4: Taisyklių grupės sukurimas



Pav. 5: Naujos grupės parametrai

Sukūrus grupę, galima pridėti taisykles (jei nėra jokios taisyklės, bus rodomi visi pažeidėjai atitinkantys grupės pagrindinius parametrus). Du kartus kairiu pelės mygtuku paspaudus ant norimos grupės bus matoma taisyklių lentelė. Dešiniu pelės mygtuku paspaudus ant lentelės atsiranda meniu, kuriame yra pasirinkimai sukurti taisyklę (Pav.) arba ištrinti esamą, jei paspausta ant egzistuojančios taisyklės eilutės. Visi vienoje taisyklėje nurodyti parametai turi atitikti ar viršyti įvykius užregistruotus tam tikram IP, salygos tikrinamos kaip loginis „IR“. Pvz.: jei pažeidėjas atliko tik 10 bandymų jungtis per SSH į sensorių A ir nieko kito, o taisyklė nurodo SSH >= 3 ir sensoriaus pavadinimas B, tai IP nepateks į filtruojamų adresų lentelę pagal šią taisyklę, jei nebuvo jokių įvykių į sensorių B (nebūtinai SSH). Atskiros taisyklės grupėje tikrinamos kaip loginis „ARBA“ ir filtravimo lentelėje bus nurodytos visos atitinkačios taisyklės.

Taisyklės parametrai, kurie bus lyginami su kiekvienu IP iš pažeidėjų lentelės:

Taisyklės pavadinimas – taisyklės pavadinimas ar trumpas aprašymas.

Įvykis – konkretaus įvykio pavadinimas (SSH, httpd, Scan: tcp 1000). Įvykių pavadinimus galima rasti detalios infromacijos apie pažeidėjus lentelėje. Įvykiai turi būti tikslūs, paieška nėra vykdoma su dalimi pavadinimo. Taip pat reikia nurodyti, kiek šito įvykio atvejų buvo užregistruota. Galima pridėti kiek tik norima įvykių.

Sensorius – konkretaus sensoriaus ID (matomas sensorių sąrato skiltyje) ir jo užfiksuotų įvykių kiekis. Galima pridėti kelis sensorius.

Sensoriaus IP – konkretaus sensoriaus IP adresas ir šį IP adresą palietusių įvykių kiekis. Galima pridėti kelis adresus.

LAN IP – kitas tinklo IP adresas, į kurį nukreiptus įvykius užfiksavo tame pačiame potinklyje esantis sensorius. Galima nurodyti kelis adresus.

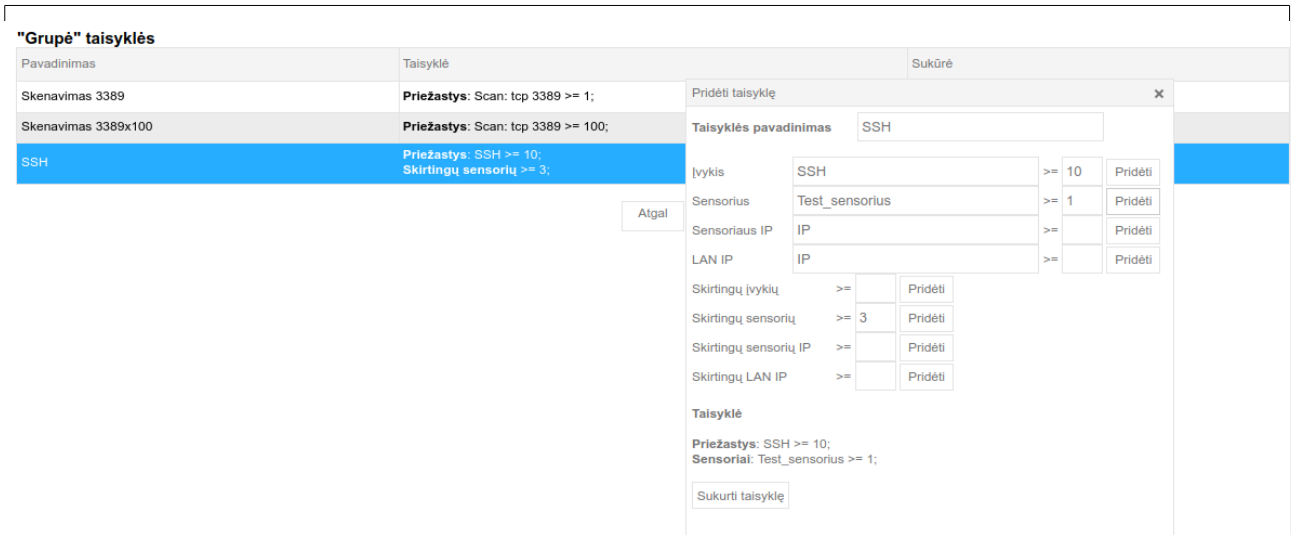
Skirtingų įvykių – bendras visų užfiksuotų įvykių kiekis.

Skirtingų sensorių – kiek skirtingų sensorių užfiksavo įvykius iš šio pažeidėjo IP.

Skirtingų sensorių IP – į kiek skirtingų sensorių IP buvo nukreipti paketai iš šio IP.

Skirtingų LAN IP – į kiek skirtingų kitų tinklo IP buvo nukreipti paketai iš šio IP.

Įrašius norimo lauko duomenis spaudžiamas šalia esantis mygtukas „Pridėti“ ir langelio apačioje matoma formuojama taisyklė. Pridėjus visus parametrus spaudžiamas mygtukas „Sukurti“ ir nauja taisyklė bus pridėta į sąrašą, jei nebuvo padaryta klaidų ir naudotojas turi tinkamas teises.



Pav. 6: Taisyklių kūrimas

Peržiūrėti taisykle atitinkančius IP adresus taisyklių grupių lentelėje reikia paspausti mygtuką „Rodyti“, kuri yra kiekvienos grupės eilutės dešinėje. Lentelėje rodomas IP adresas, paskutinio įvykio data ir atitinkančių grupės taisyklių pavadinimai. Paspaudus kairiu pelės mytuku ant įrašo lango apačioje rodoma detali informacija apie visus šio IP įvykius, kaip ir pažeidėjų lentelėje. Taisykles atitinkančių IP lentelės duomenis galima išsaugoti, kaip ir pažeidėjų lentelės, norimu formatu. Pasirinkimas yra lentelės apačioje, dešinėje pusėje. Šią informaciją galima gauti ir iš duomenų bazės, jei norima automatizuoti IP adresų blokavimą. Su APGS administratoriumi suderinus grupės pavadinimą, šaltinio IP adresą, galima filtruotų IP adresų informaciją gauti tiesiai iš Postgresql duomenų bazės.

2.3. Baltasis ir potinklių sąrašai

Baltąjame sąraše nurodyti IP adresai ar potinkliai nebus rodomi filtruojamų IP adresų lentelėje, tačiau bus rodomi pažeidėjų lentelėje ir statistika apie įvykius bus kaupiama. Potinklių sąrašas yra skirtas aprašyti kitus savo institucijos IP/potinklius, kurie nėra baltajame sąraše, bet įvykiai iš jų nebūtų matomi kitoms institucijoms. Statistika ir įvykius iš baltojo ir potinklių sąrašų matys tik juos sukūrusios institucijos naudotojai, nebent jie bus užfiksuoti kitos institucijos sensoriaus (Lentelė 1).

IP adresas	**Matomas pažeidėjų lentelėje**	**Matomas grupės filtro lentelėje**	**Matomas kitos institucijos pažeidėjų/filtrų lentelėse**	**Matomas kitos institucijos pažeidėjų/filtrų lentelėse, jei buvo užregistruoti jos sensorių**
Nėra jokiame sąraše	Taip	Taip	Taip	Taip
Baltąjame sąraše	Taip	Ne	Ne	Taip, tik tos institucijos užregistruoti įvykiai
Potinklių sąraše	Taip	Taip	Ne	Taip, tik tos institucijos užregistruoti įvykiai

Lentelė 1: Informacija apie IP adresus tarp institucijų

3. Įvykiai

Lentelės apie įvykius iš sensoriuose veikiančių tarnybų. Rodomi paskutiniai 1000 įrašų iš visų sensorių (arba tik naudotojo institucijos sensorių, jei tai pasirinkta nustatymuose). Rodoma detali informacija apie kiekvieną įvykį: prisijungimo vardas ir salpažodis, jei bandyta prisijungti prie sensoriaus, protokolo tipas, prievadų numeriai ir kita informacija.

4. Sensoriai

Sensorių skiltyje rodoma institucijos sensorių lentelė, kurioje ant sensoriau eilutės paspaudus kairiu pelės mygtuku galima atlikti veiksmus:

Parametrai – sensoriaus pavadinimo, savininko, padalinio keitimas. Visų laukų užpildyti nebūtina, tik norimus pakeisti.

Įjungti/išjungti tarnybas – galima sustabdyti atskiras tarnybas ir nebekaupti jų informacijos (pvz. palikti tik SSH imituojančią tarnybą ir nestebėti kitų tinklo paketų). Atidarytame lange (Pav. 7) galima nuimti/uždėti varneles ir išsaugoti pakeitimus.

Perkrauti sensorių

Ištrinti sensorių – pašalinti sesnorių iš sąrašo. Tai nereiškia, kad iš jo informacija nebebus renkama. Sensorių perkrovus jis automatiškai atsiras sąraše, tik be pavadinimo ir institucijos, padalinio parametrų.

Pav. 7: Sensoriaus tarnybos

5. Naudotojų rolės ir teisės

Yra keturi naudotojų lygiai: sistemos administratorius, institucijos administratorius, stebėtojas, admin stebėtojas.

Sistemos administratorius gali keisti visų sensorių parametrus, taip pat turi tiesioginę prieigą prie duomenų bazės ir gali keisti, kurti visus duomenis sistemoje. Likusios trys rolės turi prieigą tik prie Web aplikacijos https://apgs.linet.vu.lt.

Institucijos administratoriui ir stebėtojui galima nurodyti padalinius, kuriuos jis galės matyti. Jei jie nenurodyti, matomi visi institucijos sensoriai. Admin stebėtojas gali matyti visą informaciją iš sensorių iš visų institucijų. Lentelėje apačioje nurodomos kiekvienos rolės funkcijos ir teisės.

Rolė	**Matomi pažeidėjai**	**Taisyklių kūrimas**	**Baltojo/potinklio sąrašo pildymas**	**Matomi įvykiai**	**Sensorių parametrų keitimas ir peržiūra**
Sistemos administratorius	Visi	Taip	Taip	Visi	Taip, visų intitucijų
Admin stebėtojas	Visi	Negalimas, tik peržiūra savo institucijos taisyklių	Negalimas, tik peržiūra savo institucijos taisyklių	Visi	Tik peržiūra, visų institucijų
Institucijos administratorius	Savo institucijos (padalinio) ir ribotai iš kitų sensorių	Taip, savo institucijos (padalinio)	Taip,savo institucijos (padalinio)	Savo institucijos (padalinio) ir ribotai iš kitų sensorių	Taip, tik savo institucijos (padalinio)
Stebėtojas	Savo institucijos (padalinio) ir ribotai iš kitų sensorių	Negalimas, tik peržiūra savo institucijos (padalinio) taisyklių	Negalimas, tik peržiūra savo institucijos (padalinio) taisyklių	Savo institucijos (padalinio) ir ribotai iš kitų sensorių	Tik peržiūra, savo institucijos (padalinio)

Lentelė 2: Rolės ir jų teisės