„Dirbtinio intelekto metodų taikymas įsiskverbimų į kompiuterinius tinklus aptikimo sistemose.“

2016–2020 m. studijos

Doktorantas: Liudas Ališauskas
Vadovas: Virginijus Marcinkevičius

Disertacijos tikslas ir objektas

Tyrimo tikslas:

Pagerinti dirbtinio intelekto metodų rezultatų tikslumą ir efektyvumą aptinkant įsiskverbimus į kompiuterinius tinklus.

Tyrimo objektas:

Dirbtinio intelekto metodai, jų rezultatų tikslumas ir efektyvumas aptinkant įsiskverbimus į kompiuterinius tinklus.

Disertacijos tikslas ir objektas

Tyrimo uždaviniai:

- Atlikti kompiuterinių tinklų duomenų srauto ir veiklą registruojančių įrašų analizę.
- Atlikti įsiskverbimų į kompiuterių tinklus atakos vektorių analizę.
- Atlikti dirbtinio intelekto metodų taikomų aptinkant įsiskverbimus į kompiuterių tinklus analizę.

Planuojami rezultatai:

- Kompiuterinių tinklų veiklą atspindinčių duomenų struktūras.
- Įsiskverbimų į kompiuterių tinklus požymiai, kurių pagalba mokomi dirbtinio intelekto metodai.
- Nustatyti šiuo metu kompiuterių tinklų saugos sprendimuose taikomi dirbtinio intelekto metodai, jų taikymo aplinkybės.

2017–2018 m. m. darbo planas

Studijų planas:

- Išlaikyti egzaminą „Lygiagretieji ir paskirstytieji skaičiavimai“. Vertinimo komisija: prof. dr. Julius Žilinskas, doc. dr. Algirdas Lančinskas, dr. Viktor Medvedev.

Mokslinių tyrimų planas:

- Atlikti teorinius ir praktinius tyrimus toliau sprendžiant dirbtinio intelekto metodų, taikymų įsiskverbimų į kompiuterinius tinklus aptikimo sistemose, tikslumo ir efektyvumo uždavinį;
- Tyrimo metodikos sudarymas:
  - Problemų kylančių iš tikslo suformulavimas būsimiems eksperimentiniams ir analitiniams tyrimams.
  - Uždavinių skirtų nustatytoms problemoms spręsti aprašymas.
  - Tinkamos tyrimo metodikos parinkimas iškeltiems uždaviniams spręsti. (Sukurta tyrimų laboratorija)
  - Teorinio ir empirinio tyrimų suplanavimas pagal pasirinktą metodiką.

2017–2018 m. m. darbo planas

Rezultatų pristatymo planas:

- Dalyvauti tarptautinėje mokslinėje konferencijoje Lietuvoje pristatant teorinio tyrimo rezultatus.

Mokslinių publikacijų planas:

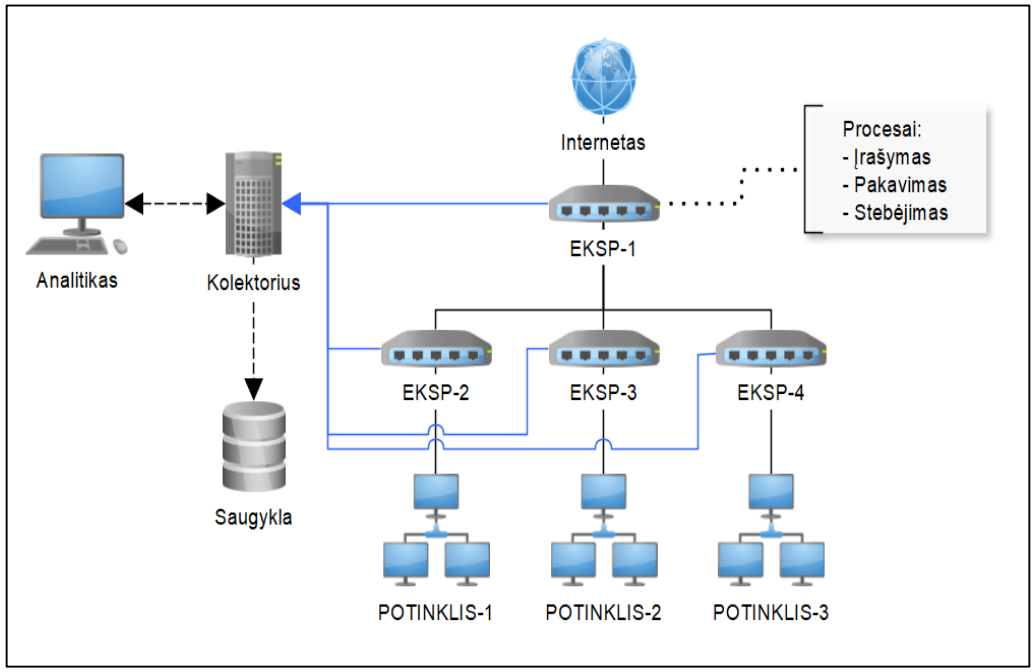
- Publikuoti dirbtinio intelekto metodų taikymo įsiskverbimų į kompiuterinius tinklus aptikimo sistemose tyrimo rezultatus tarptautiniame recenzuojamame leidinyje.

Problemų kylančių iš tikslo suformulavimas būsimiems eksperimentiniams ir analitiniams tyrimams.

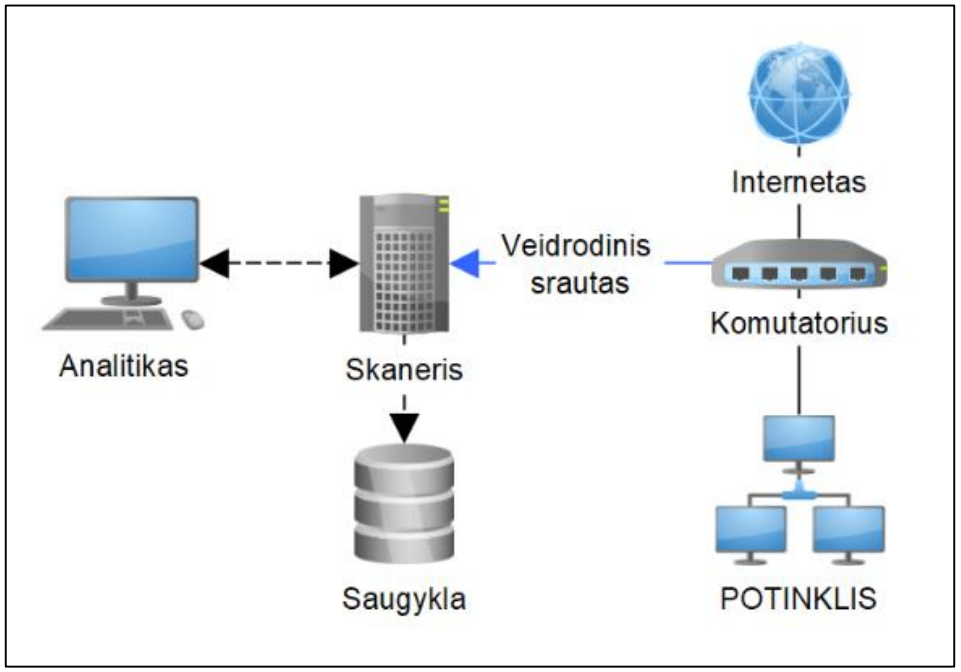
- Tyrimo srities mokslinių straipsnių analizė:
  - Daugelis jų stokoja informacijos kai būtų galima pakartoti tyrimus.
  - Nėra viešai prieinami tyrimuose naudoti duomenys.

- Viešai publikuojami tyrimui aktualūs duomenų rinkiniai:
  - Skirtingi duomenų formatai
  - Nėra duomenų realiuoju laiku

Kompiuterių tinklo srauto duomenys



Principinė tinklo srautų analizės technologijų schema.



Principinė tinklo srauto nuskaitymo schema.

Kompiuterių tinklo srauto duomenys

@timestamp	SIP	SP	DIP	DP	Proto	Pkts	SBytes
August 10th 2011, 12:49:53.776	10.32.84.229	13363	78.51.177.141	31204	udp	8	292
August 10th 2011, 12:49:32.314	86.176.213.5	18089	10.32.84.229	13363	udp	4	154
August 10th 2011, 12:49:53.776	10.32.84.229	13363	90.9.234.17	36850	udp	4	539
August 10th 2011, 12:49:32.338	10.32.84.229	13363	98.185.51.118	5795	udp	3	180
August 10th 2011, 12:49:53.776	10.32.84.229	13363	82.81.237.213	16192	udp	18	1,002
August 10th 2011, 12:49:32.341	92.244.234.117	10679	10.32.84.229	13363	udp	14	1,085
August 10th 2011, 12:49:53.783	168.167.65.254	4750	10.32.84.229	13363	udp	2	188
August 10th 2011, 12:49:32.341	202.62.103.38	26267	10.32.84.229	13363	udp	14	1,980
August 10th 2011, 12:49:53.805	212.93.105.18	23970	10.32.84.229	13363	udp	2	72
August 10th 2011, 12:49:32.345	95.86.117.254	1026	10.32.84.59	6881	udp	1	107

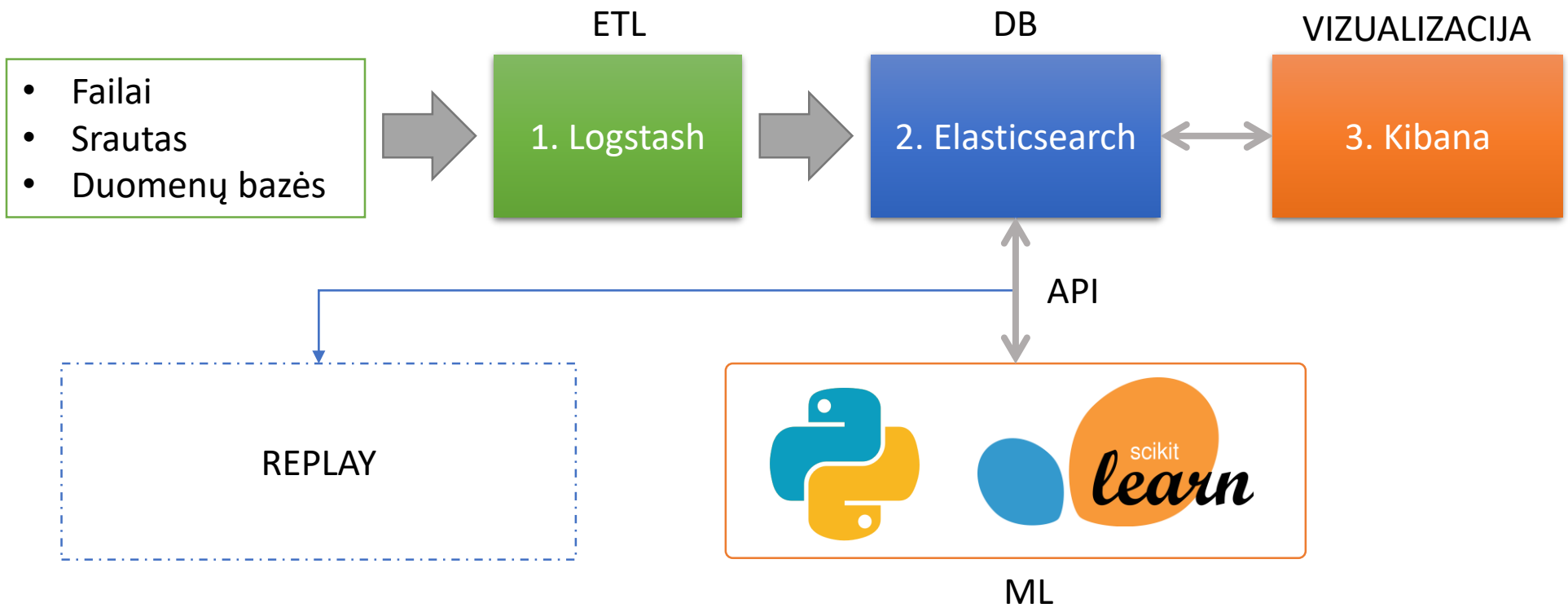
Principinė kibernetinės atakos schema

- 1 etapas: Žvalgyba (angl. Reconnaissance)
- 2 etapas: Pirminis įsilaužimas (angl. Initial compromise)
- 3 etapas: Vadovavimas ir valdymas (angl. Command & control)
- **4 etapas: Horizontalus judėjimas (angl. Lateral movement)***
- 5 etapas: Taikinių užvaldymas (angl. Target attainment)
- 6 etapas: Duomenų ištraukimas, sistemų sugadinimas ir sutrikdymas (angl. Exfiltration, corruption, and disruption)

Visi žingsniai palieka pėdsakus.

* Tolimesnė tyrimų sritis

Laboratorija



Laboratorija

Ataskaitinių metų rezultatai

- Išlaikyti egzaminai:
  - „Lygiagretieji ir paskirstytieji skaičiavimai“. Vertinimo komisija: prof. dr. Julius Žilinskas, doc. dr. Algirdas Lančinskas, dr. Viktor Medvedev. (Papildyti praktinę dalį, pateikti ataskaitą.)
- Sukonstruota laboratorija.
- Nesudalyvauta tarptautinėje konferencijoje ir nepublikuotas straipsnis. (Vertingų rezultatų stoka)

Dėkoju už dėmesį