

IS lietotāju aizdomīgo darbību identifikācija:

 *-StepControl* risinājuma pieeja

Identifying suspicious activities

Dr.sc.ing. Vitālijs Zabiņako

Zinātnisko pētījumu un produktu
attīstības departaments

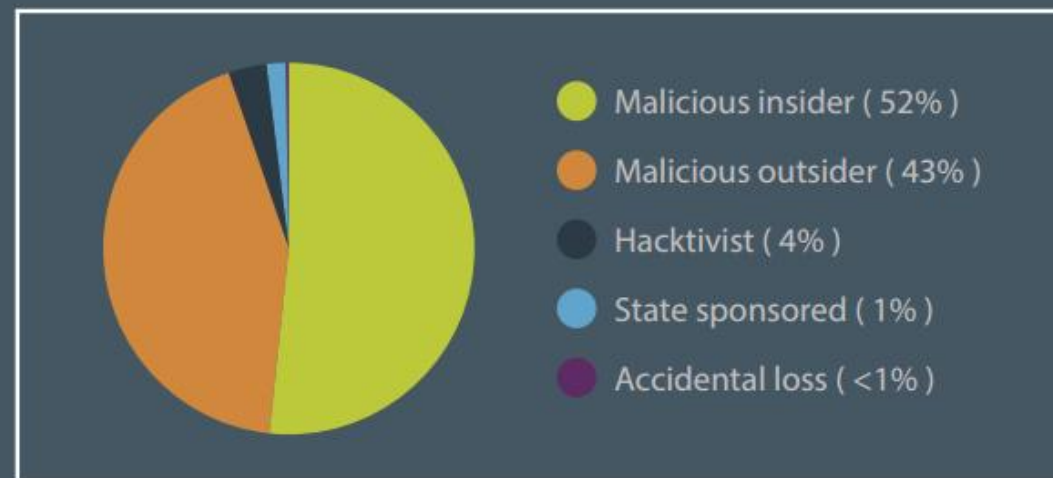
Prezentācijas saturs

- ✓ Iekšējo draudu ietekme modernajās IT sistēmās
- ✓ Risinājums “e-StepControl”:
 - Arhitektūra
 - Pieeja
 - Lietotāja grafiskā saskarne
 - Raksturojumi
- ✓ Secinājumi un attīstība

Iekšējo draudu ietekme

1. <http://breachlevelindex.com/pdf/Breach-Level-Index-Report-Q12014.pdf>
2. <http://enterprise-encryption.vormetric.com/rs/vormetric/images/Global-Insider-Threat-WEB.pdf>
3. <http://www.vormetric.com/campaigns/insiderthreat/2015/pdf/2015-vormetric-insider-threat-press-deck-v3.pdf>
4. https://www.forcepoint.com/sites/default/files/resources/files/whitepaper_insider_threat_federal_en_0.pdf
5. http://enterprise-encryption.vormetric.com/rs/480-LWA-970/images/2015_Vormetric_ITR_European_R3.pdf

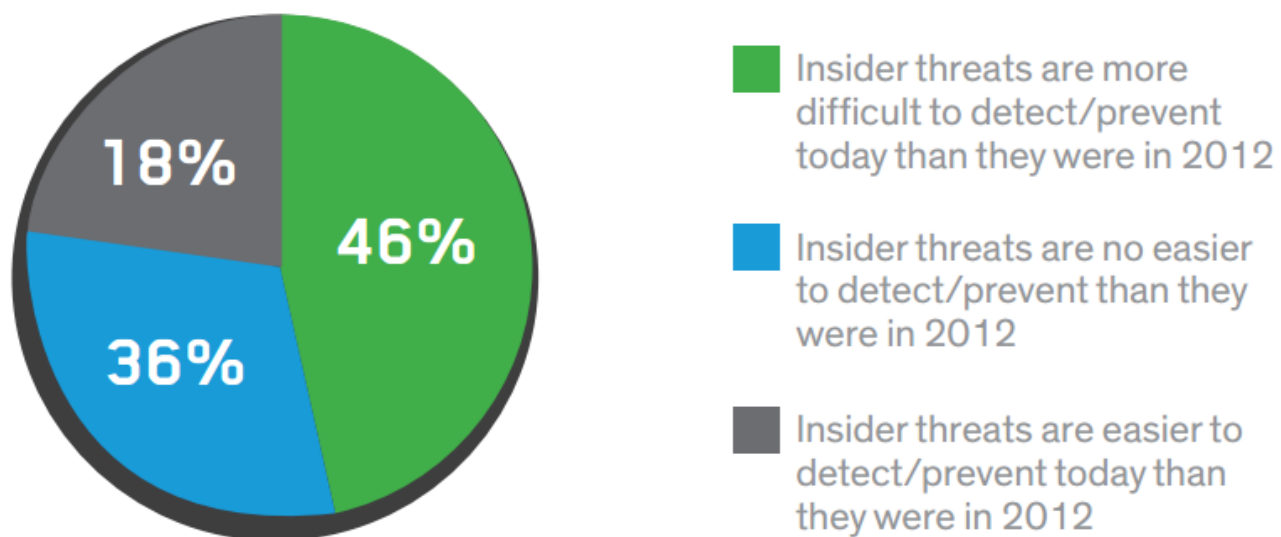
TOP BREACH RECORDS BY SOURCE



Malicious insiders claimed the top spot for number of records breached in the first quarter of 2014, accounting for 52% of total number of data records breached. This was followed by malicious outsiders (43%), hactivists (4%), state sponsored (1%), and accidental loss of data (<1%).

Iekšējo draudu ietekme

Figure 2: How European organizations view the difficulty in identifying insider threats



Avots [2]

Iekšējo draudu ietekme

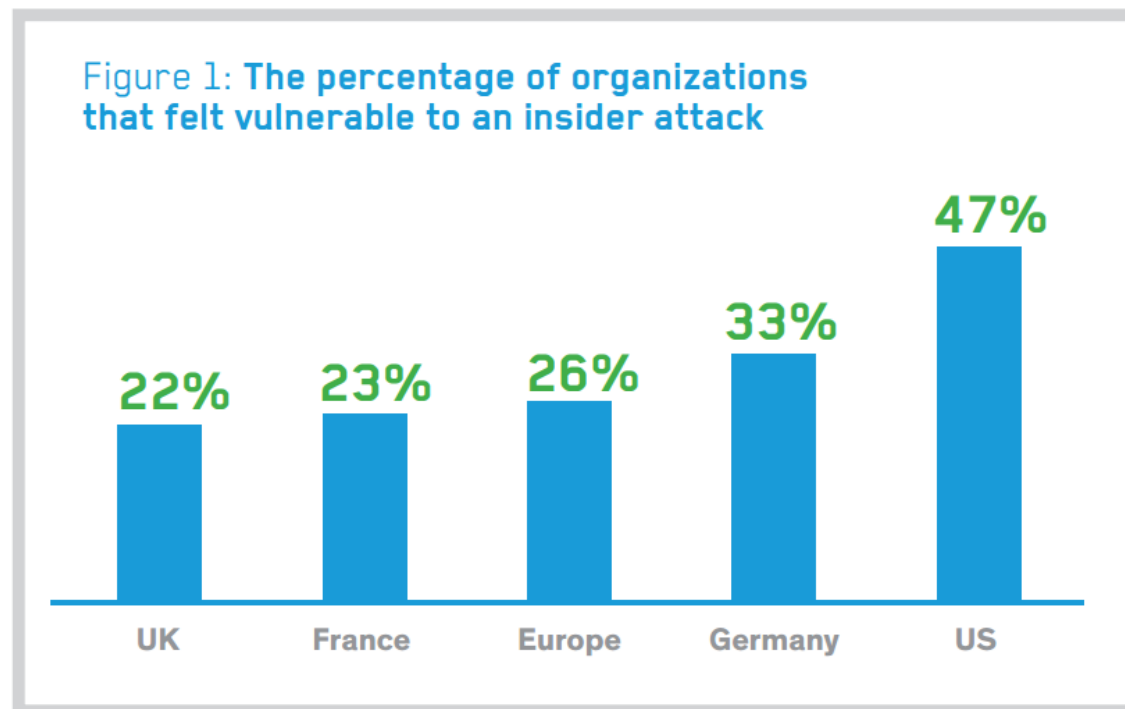
Figure 3: The top 4 reasons why insider threats are more difficult to detect

- 1 The growing volume of network activity
- 2 The growing use of cloud computing
- 3 There are more employees, contractors, business partners, etc. with access to our network
- 4 We have more IT assets on the network which makes security more difficult

Avots [2]

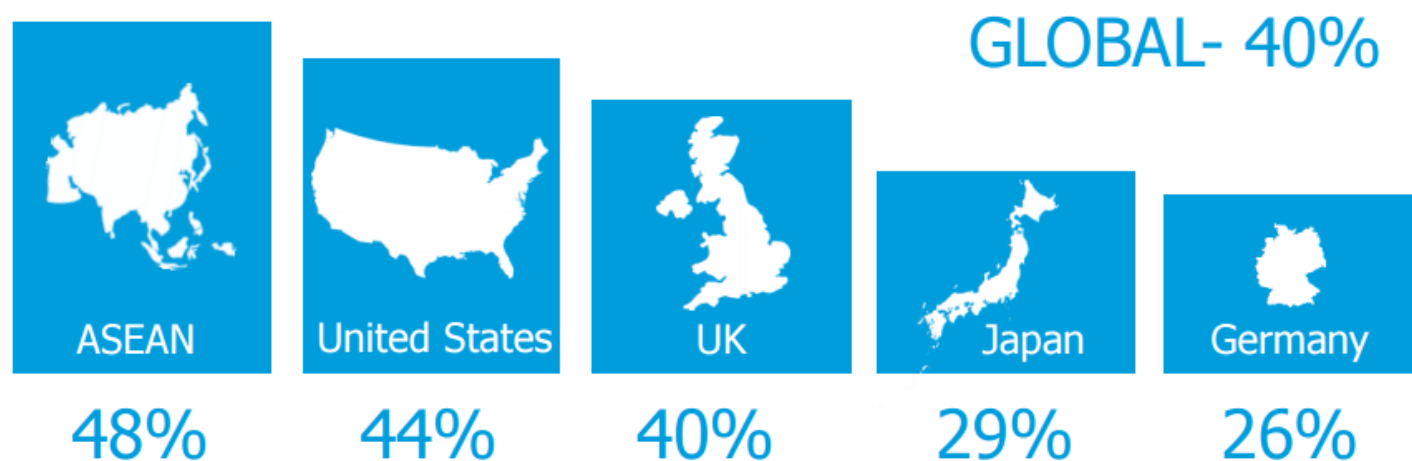
Iekšējo draudu ietekme

Figure 1 below identifies the European position on vulnerability to insider attacks. It shows that the European country feeling most vulnerable to the threat was Germany at 33%, with France and the UK both returning figures of 23% and 22% respectively. This contrasted to an earlier US survey from September 2013 which showed that a massive 47% of US respondents felt vulnerable to insider attacks.



Avots [2]

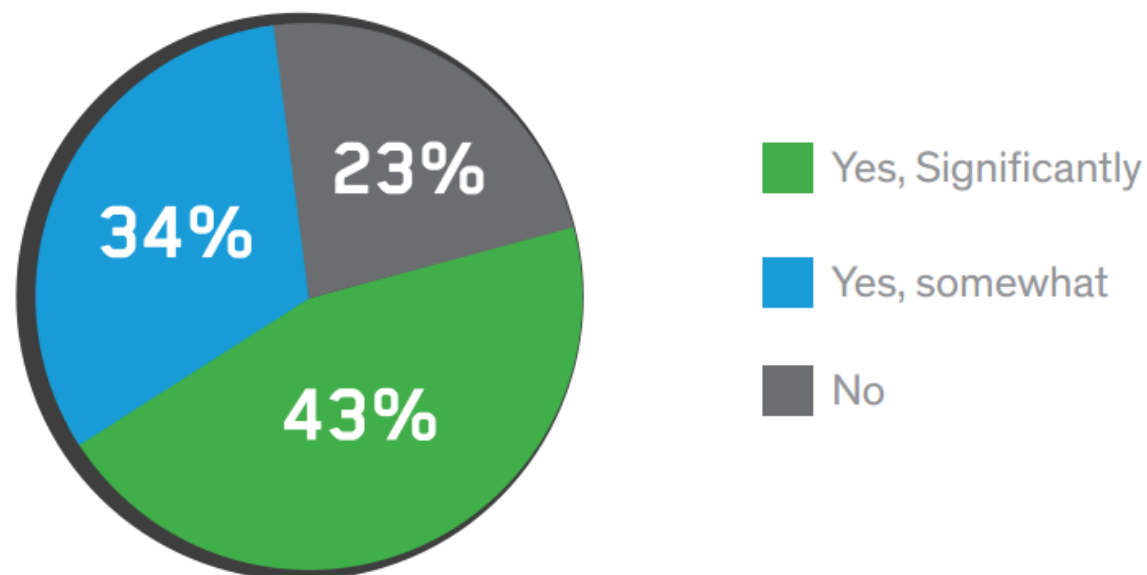
Iekšējo draudu ietekme



**EXPERIENCED A DATA BREACH
OR FAILED A COMPLIANCE AUDIT**

Iekšējo draudu ietekme

Figure 5: The percentage of organizations planning security budget increases as a result of insider attacks



Iekšējo draudu ietekme

INSIDER THREATS HOW TO PROTECT YOUR DATA



**CONCENTRATE ON PROTECTING
DATA AT THE SOURCE**



**MAKE ENCRYPTION WITH ACCESS
CONTROLS THE DEFAULT**



**MONITOR AND ANALYZE DATA
ACCESS PATTERNS**



**REPLACE POINT SOLUTIONS WITH
DATA SECURITY PLATFORMS**

Piedāvātais risinājums



Risinājuma komponentes

- Arhitektūra:

- ✓ Analizējamās IS audita adapteris
- ✓ e-SC algoritma implementācijas modulis
- ✓ Grafiskā saskarne

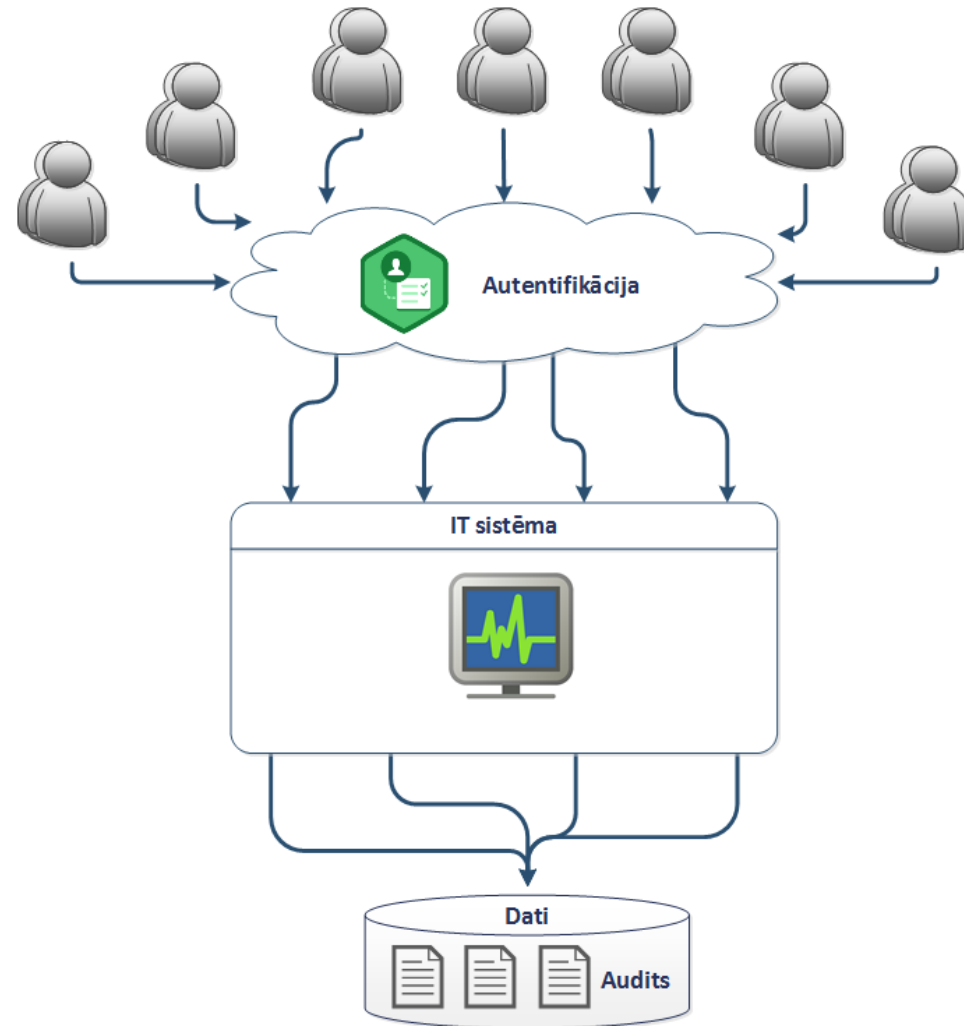
- Pieeja:

- ✓ Lietotāju darbību vēstures analīze
- ✓ e-SC apmācība, lietotāju profilu izveidošana
- ✓ Jaunu darbību “on-line” monitorings un uzraudzība

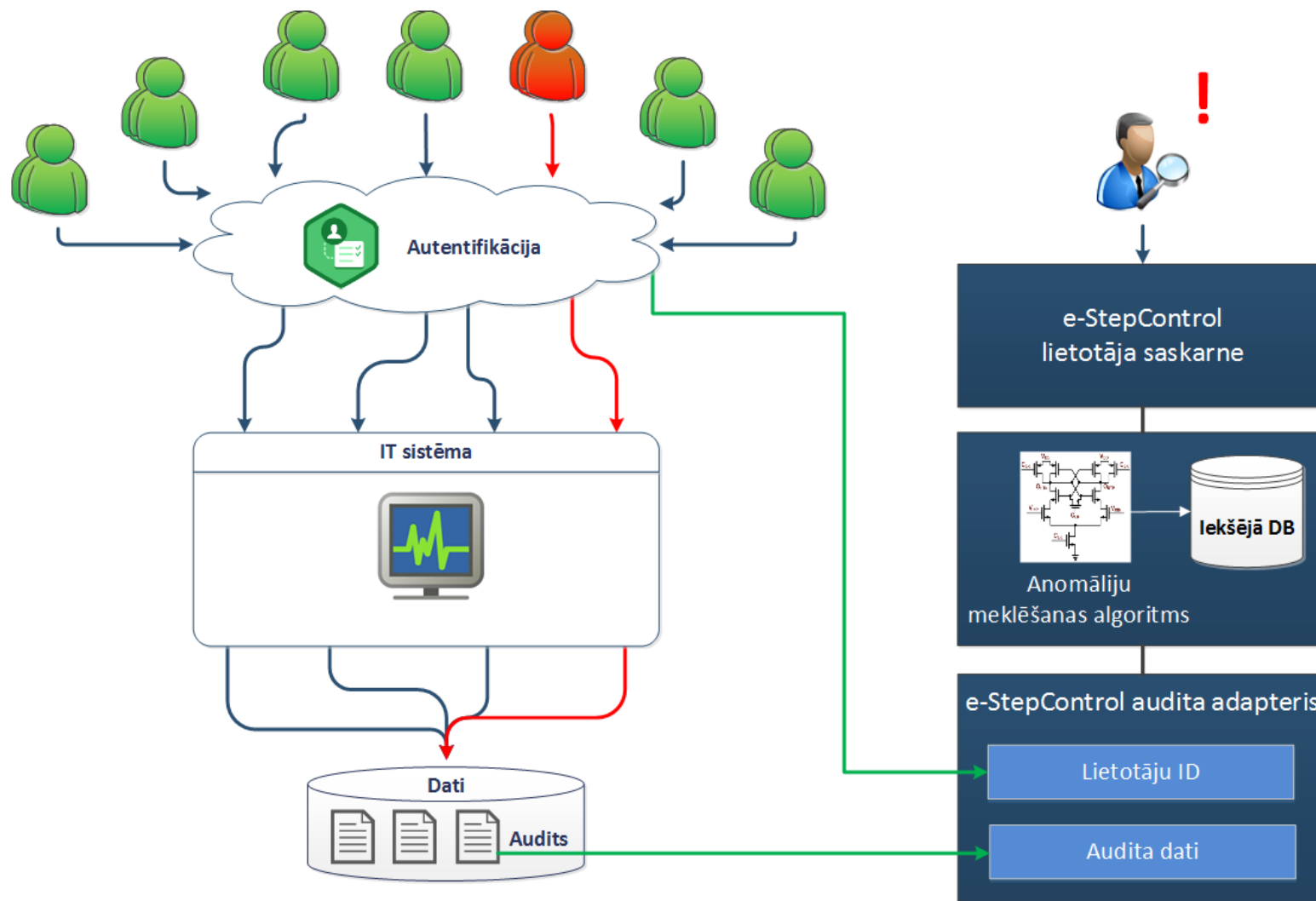
- Matemātiskais modelis:

- ✓ Grafu teorija
- ✓ Markova ķēžu princips
- ✓ Darbību aizdomīguma metrikas

Arhitektūra: IS tipveida modelis



Arhitektūra: e-SC ieviešana



Pieeja: 3 soļi

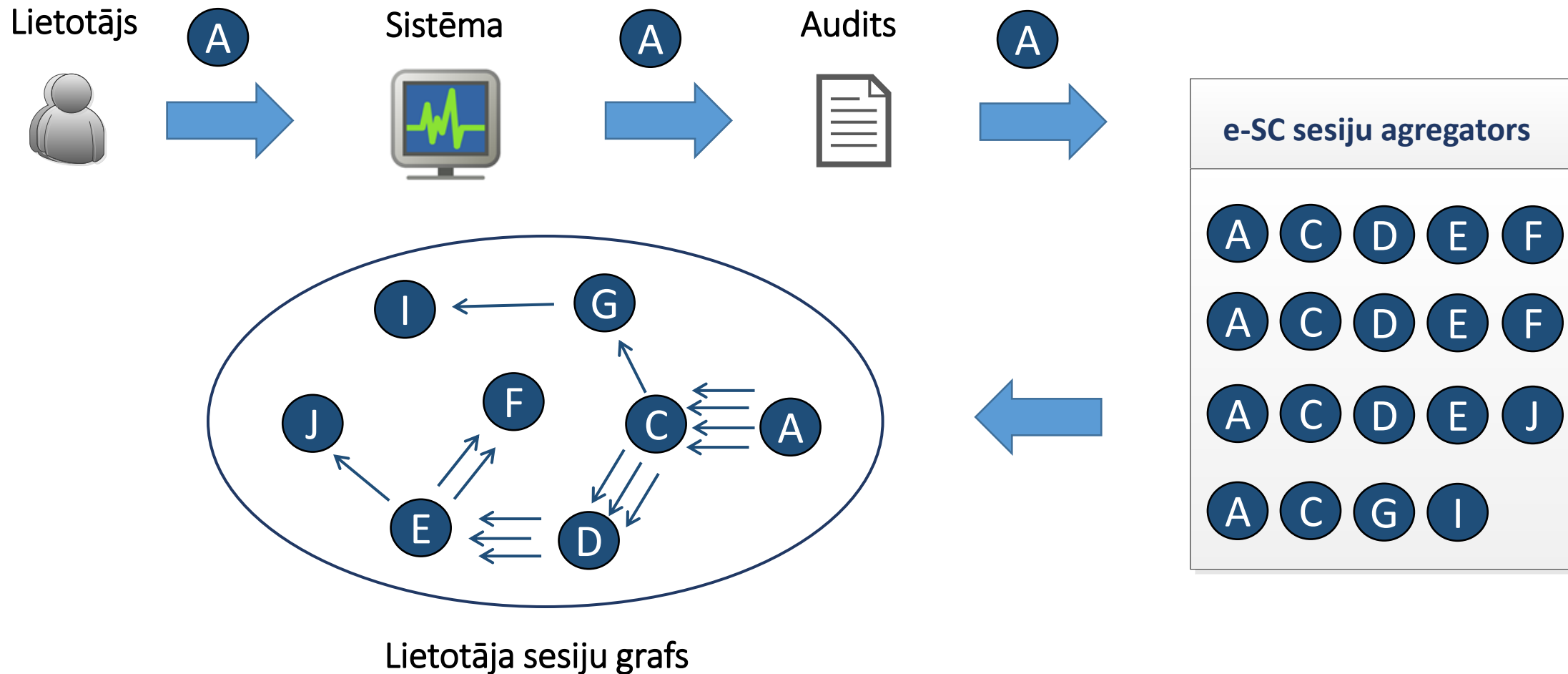
- 1. solis – pieslēgšana, datu savākšana
 - ✓ e-SC pieslēgšana ir salīdzinoši vienkārša un neprasīs papildu ieguldījumus
 - ✓ jārada iespēja lasīt datus no lietotāju darbību auditācijas pierakstiem
 - ✓ ir jānodod lietotāju identifikatori un lomas/tiesības
- 2. solis – apmācība, lietotāju profilu izveidošana
 - ✓ ir nepieciešams veikt katra lietotāja vēsturisko darbību analīzi, lai izveidotu atbilstošus uzvedības profilus
 - ✓ tiek veidoti 2 tipu profili – individuālais un grupas
- 3. solis – monitorings un uzraudzība
 - ✓ Pēc apmācības pabeigšanas e-SC turpinās veikt lietotāju darbību monitoringu „on-line” režīmā un nepieciešamības gadījumā informēs par pārkāpumiem

Pieeja: 1. solis – datu savākšana

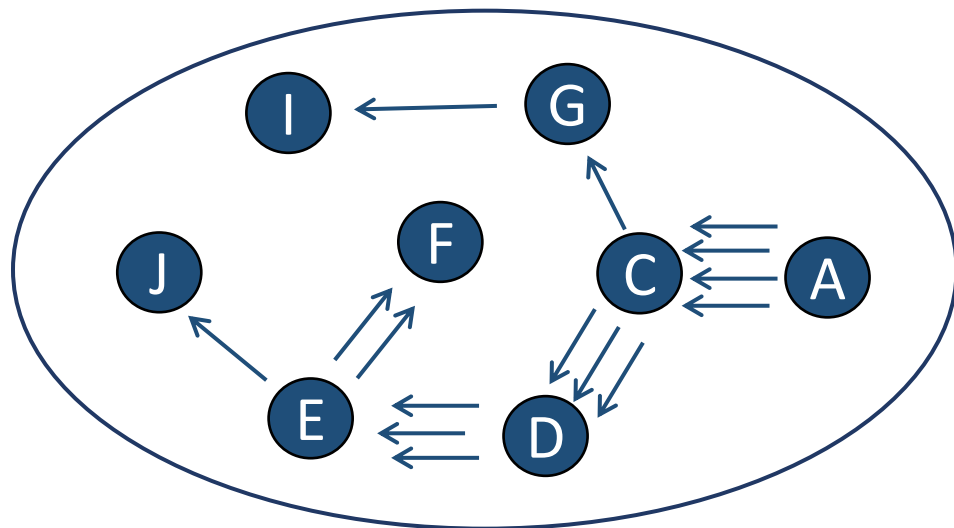
Lietotāju atomāro darbību piemēri auditācijas līmenī:

- A** – autentifikācija;
- B** – izvēlnes apskatīšana;
- C** – informācijas meklēšana;
- D** – atlasīto ierakstu rezultāta apskatīšana;
- E** – ar konkrēto personu saistīto datu rediģēšana;
- ...
- Z** – izeja no sistēmas.

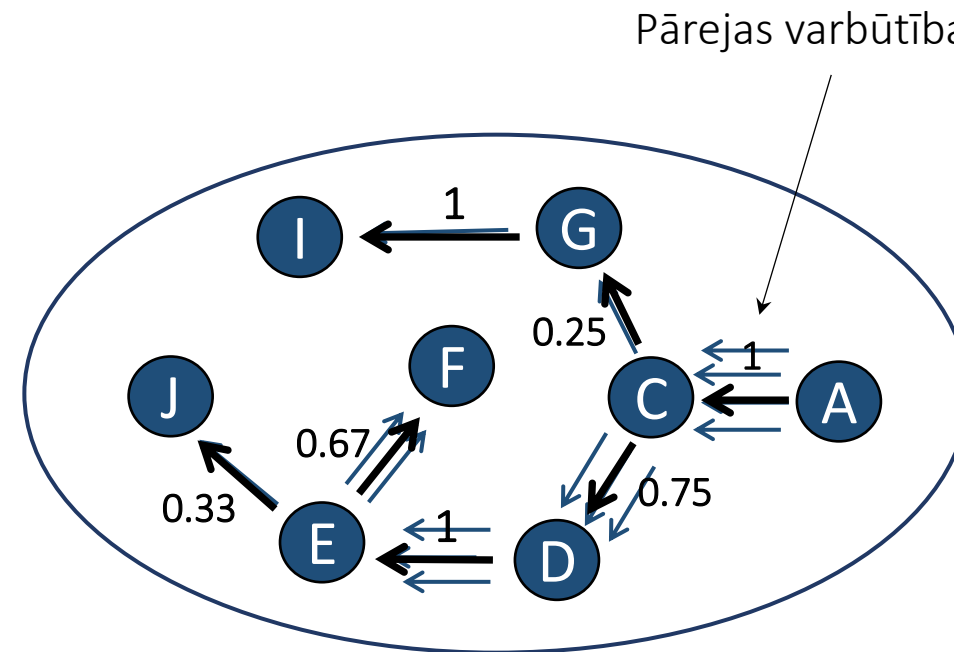
Pieeja: 1. solis – datu savākšana



Pieeja: 2. solis – profilu izveidošana



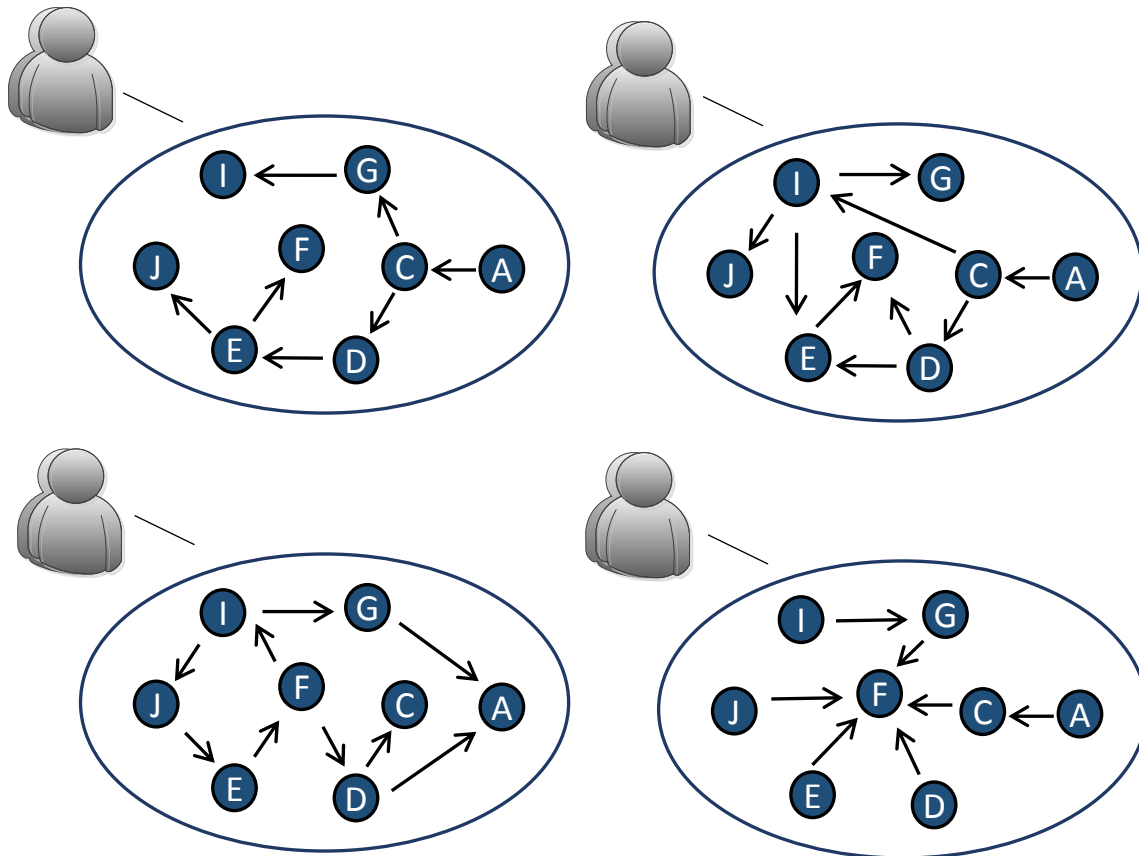
Lietotāja sesiju grafs



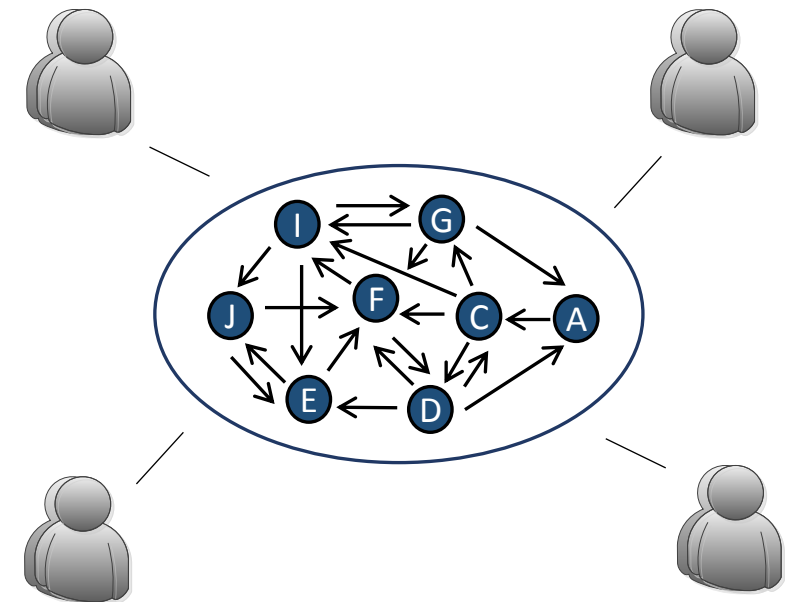
Lietotāja profila grafs

Pieeja: 2. solis – profilu izveidošana

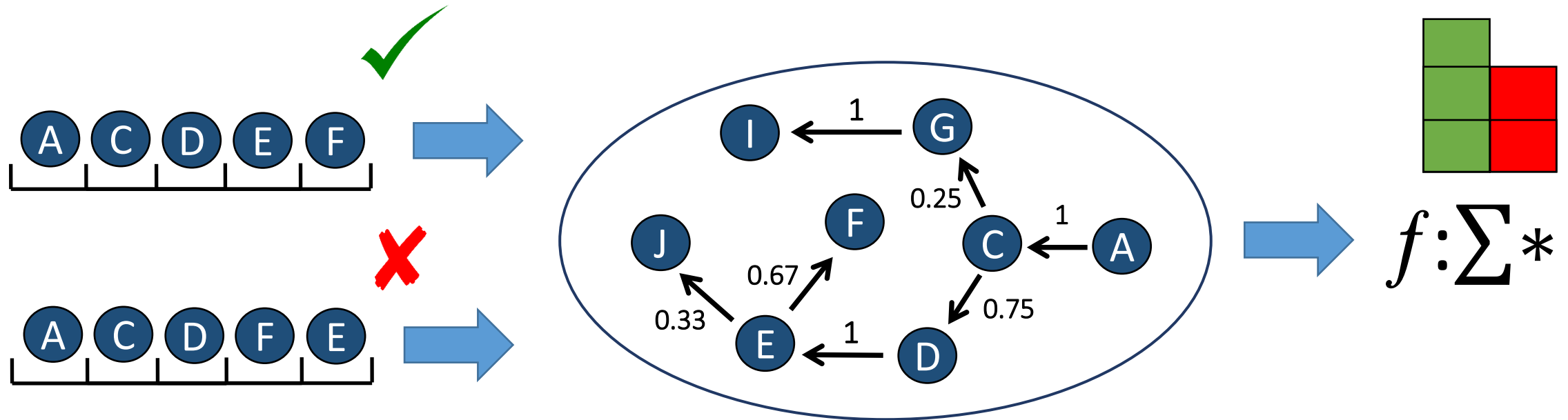
Individuālie lietotāju profili



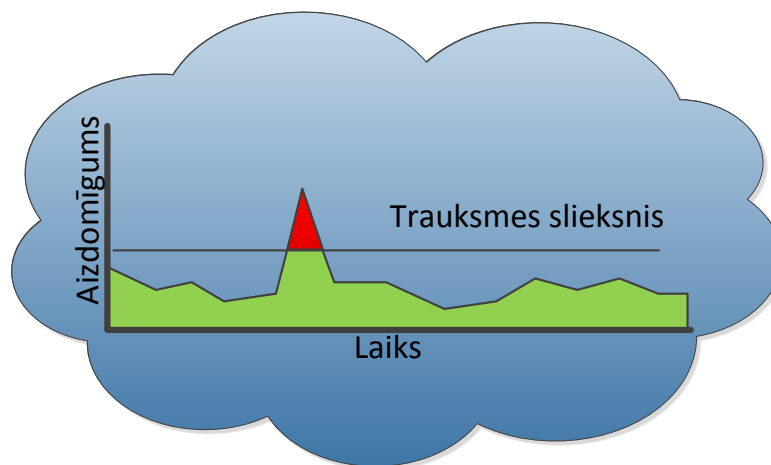
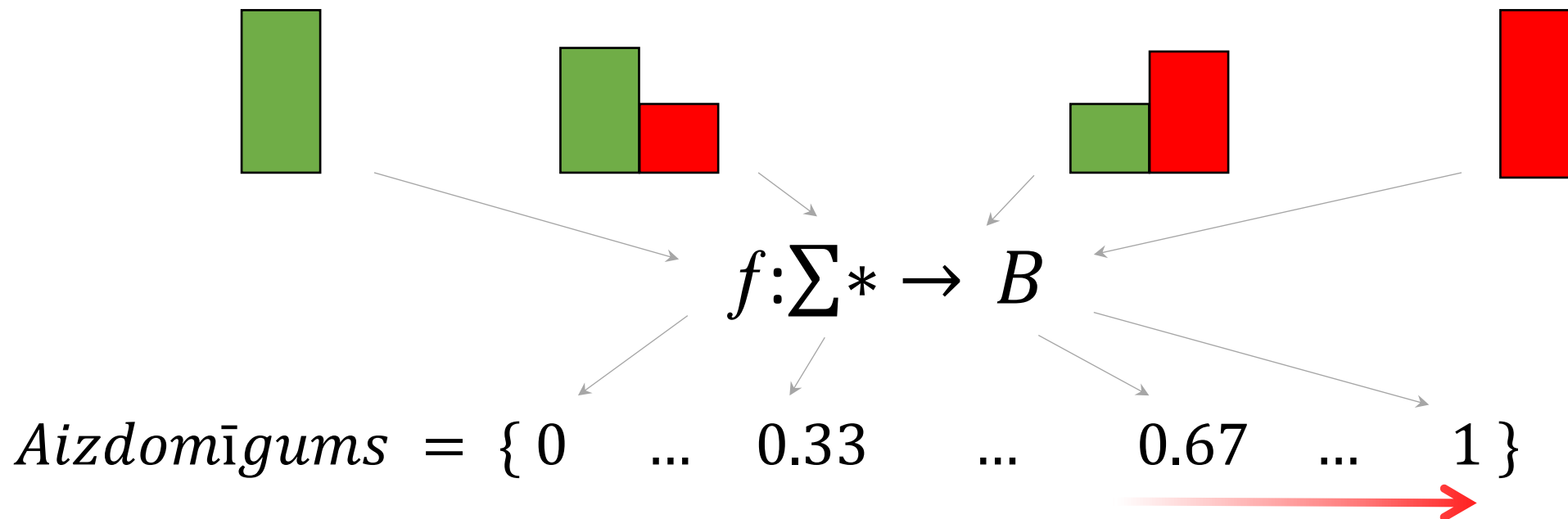
Kopējais grupas profils



Pieeja: 3. solis – monitorings

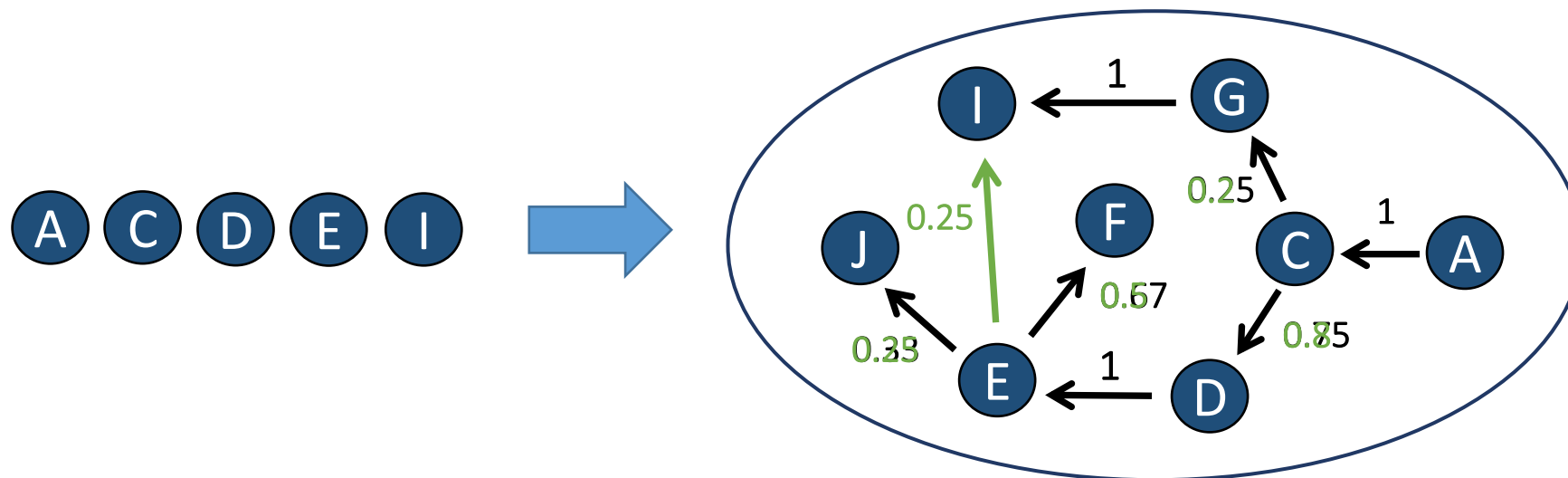


Pieejā: 3. solis – monitorings

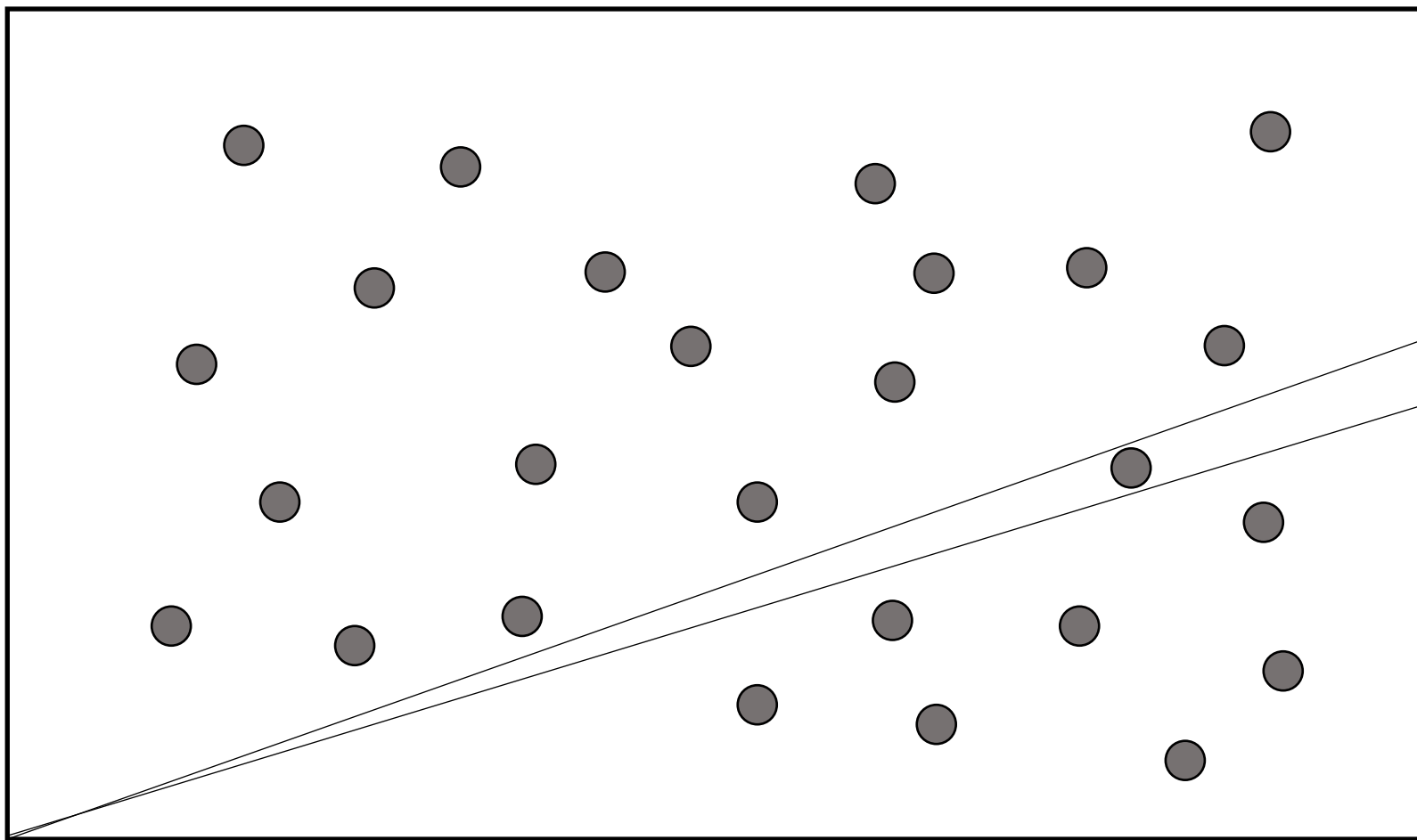


Pieeja: 3. solis – profila aktualizācija

Aizdomīgums = { 0 ... 0.33 ... 0.67 ... 1 }



Pieeja: 3. solis – profila aktualizācija



- Neizanalizētā datu kopa
- Klasifikācija ir pabeigta
- Sistēma ir apmācīta
- Pozitīvais scenārijs
- Negatīvais scenārijs
- Negatīvais scenārijs (?)
- Statusa precizējums
- Klasifikācijas korekcija

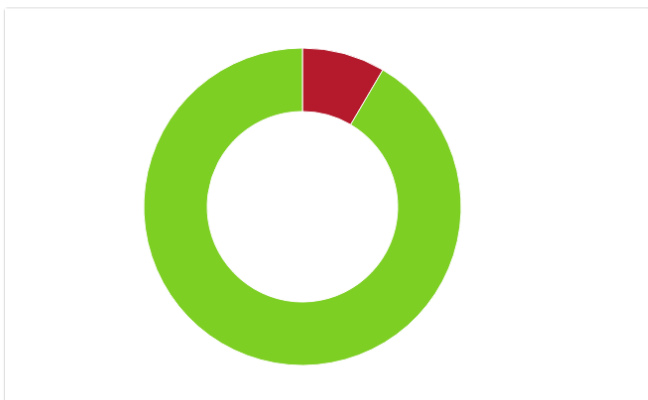
e-SC lietotāja saskarne

8% Aizdomīgs
0% Neapstrādāts
92% Tipveida

Jūlijs 5, 2016 - Augusts 3, 2016

Aizdomīgo darbību TOP5

ĢIRTS MIĶELSONS	11
TestVards TestUzvards	11
AIGARS ZUPA	9
LELDE LEJA	8
Aigars Obodovs	8



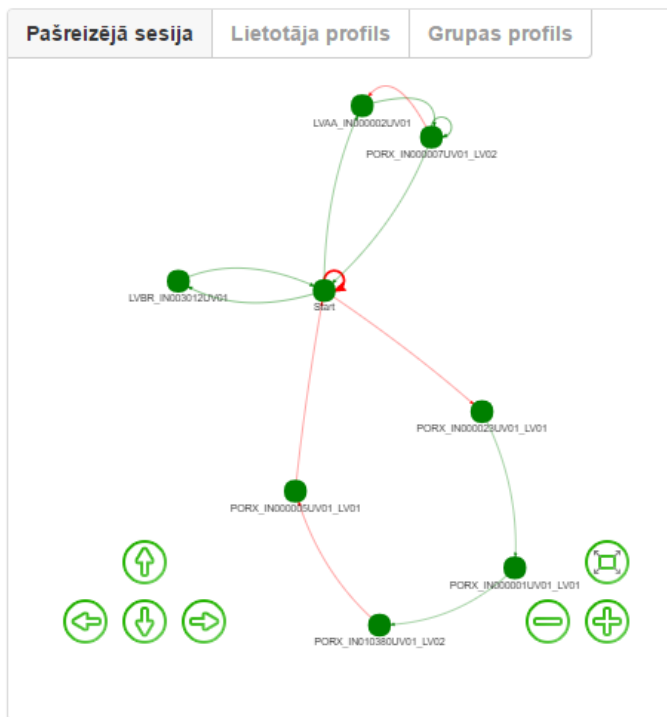
Statistika, aizdomīgo lietotāju "Top-5"

Aizdomīgs Rezervēts Pārk. noraidīts Pārk. apstiprināts ? Neapstrādāts Tipveida ? Augusts 7, 2016 - Septembris 6, 2016

Lietotāja dati	Sākuma laiks	Pabeigšanas laiks	Ilgums
● ĢIRTS MIĶELSONS	02.09.2016 14:37:03	02.09.2016 16:13:48	00.01:36:44
● LELDE LEJA	02.09.2016 16:12:56	02.09.2016 16:12:56	00.00:00:00
● AIGARS ZUPA	02.09.2016 16:03:52	02.09.2016 16:03:52	00.00:00:00
● TestVards TestUzvards	02.09.2016 16:02:20	02.09.2016 16:02:20	00.00:00:00
● JĀNIS PRIEDE	02.09.2016 15:55:44	02.09.2016 16:00:13	00.00:04:28
● TestVards TestUzvards	02.09.2016 15:37:54	02.09.2016 15:37:54	00.00:00:00
● LELDE LEJA	02.09.2016 15:34:26	02.09.2016 15:34:26	00.00:00:00
● TestVards TestUzvards	02.09.2016 15:07:23	02.09.2016 15:31:45	00.00:24:22
● ĢIRTS MIĶELSONS	02.09.2016 15:04:12	02.09.2016 15:04:12	00.00:00:00
● TestVards TestUzvards	02.09.2016 15:02:30	02.09.2016 15:02:30	00.00:00:00

Darbības sesiju saraksts

Custom Tester



Lietotāju profilu vizuālā analīze

2016.09.05. 16:08:56	PRPA_IN101307UV02_LV01	Ievaddati: Iegūt pacienta karti
2016.09.05. 16:09:05	LVPS_IN000003UV01	Apziņošanas servisa ienākošo ziņojumu pieprasījums
2016.09.05. 16:09:10	LVPS_IN000005UV01	Apziņošanas servisa izejošo ziņojumu pieprasījums
2016.09.05. 16:13:45	PRPA_IN101307UV02_LV01	Pacienta kartes iegūšana.
2016.09.05. 16:13:46	PRPA_IN101307UV02_LV01	Ievaddati: Iegūt pacienta karti
2016.09.05. 16:14:06	PRPA_IN000011UV01_LV01	Nosaukums: Izgūt pieteikuma statusu Ievaddati: Pieteikuma statusa pieprasījums
2016.09.05. 16:14:09	PRPA_IN101307UV02_LV01	Pacienta kartes iegūšana.
2016.09.05. 16:14:12	PRPA_IN101307UV02_LV01	Ievaddati: Iegūt pacienta karti

Pārk. soļus < > Noraidīt aizdomas Apstiprināt pārkāpumu Rezervēt

Pārkāpumu soļu izpēte

Apmācības režīms
Apmācīt uz tipveida darbībām

Apmācību periods
Apmācīt uzreiz

Noteikt aizdomīgu darbību
Abi (lietotājs un grupa)

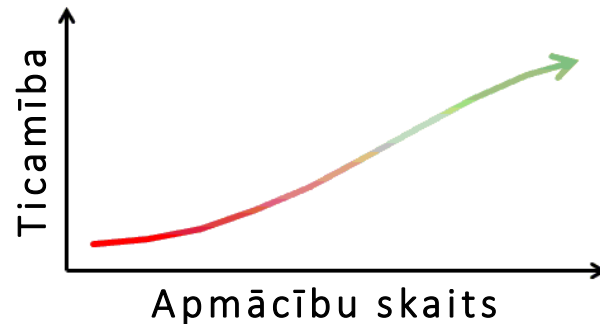
Darbību vēstures uzglabāšana
1 mēnesis

Dzešanas procesa pēdējā izpilde
0001.01.01. 0:00:00

Saglabāt

Raksturojumi un perspektīvas

- Saskaņā ar zinātnieku aprēķiniem, izmantojamā anomāliju meklēšanas metode spēj atklāt ap 85% aizdomīgām darbībām.
- Svarīgs nosacījums ir kvalitatīvā un pilna apmācību datu kopa:



- Attīstot e-StepControl risinājumu, tiek veikti turpmākie pētījumi, lai būtu iespējams analizēt arī citus lietotāju raksturojumus:
 - ✓ IP adreses;
 - ✓ piekļuves laikus;
 - ✓ utt.

Rezumējot...



IS sistēmu lietotāju pārkāpumu meklēšana ir līdzīga adatas meklēšanai degošā siena kaudzē – tik daudz siena un tik maz laika...

Rezumējot...



...taču pareizo rīku pielietošana padara šo uzdevumu par viegli atrisināmo!