IS lietotāju aizdomīgo darbību identifikācija: e-StepControl risinājuma pieeja

Identifying suspicious activities

Dr.sc.ing. Vitālijs Zabiņako

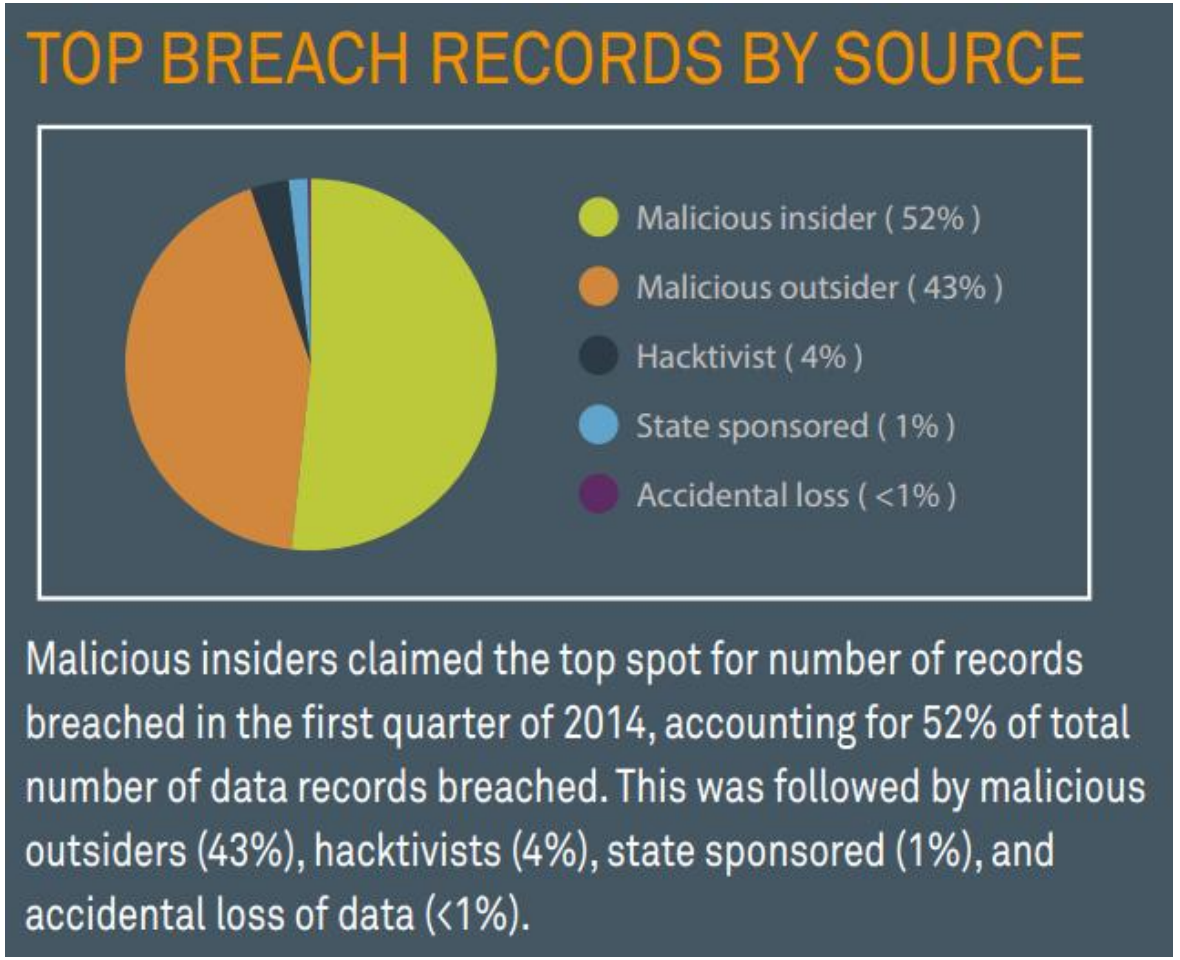
Zinātnisko pētījumu un produktu attīstības departaments

Prezentācijas saturs

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

Iekšējo draudu ietekme

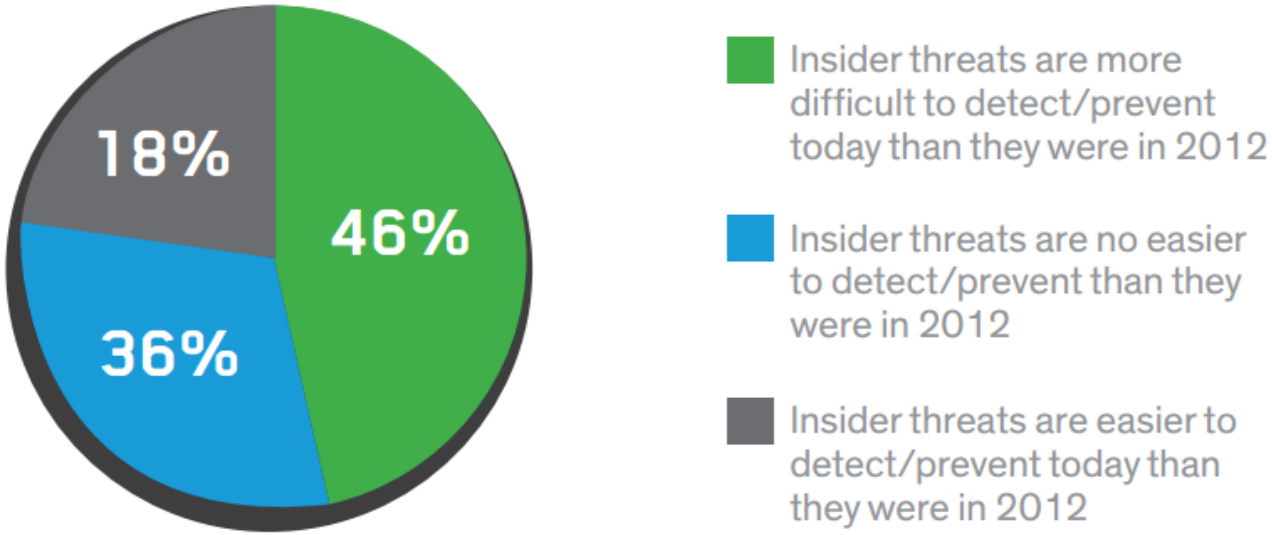
1. http://breachlevelindex.com/pdf/Breach-Level-Index-Report-Q12014.pdf
2. http://enterprise-encryption.vormetric.com/rs/vormetric/images/Global-Insider-Threat-WEB.pdf
3. http://www.vormetric.com/campaigns/insiderthreat/2015/pdf/2015-vormetric-insider-threat-press-deck-v3.pdf
4. https://www.forcepoint.com/sites/default/files/resources/files/whitepaper_insider_th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



Avots [1]

Iekšējo draudu ietekme

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



Avots [2]

Iekšējo draudu ietekme

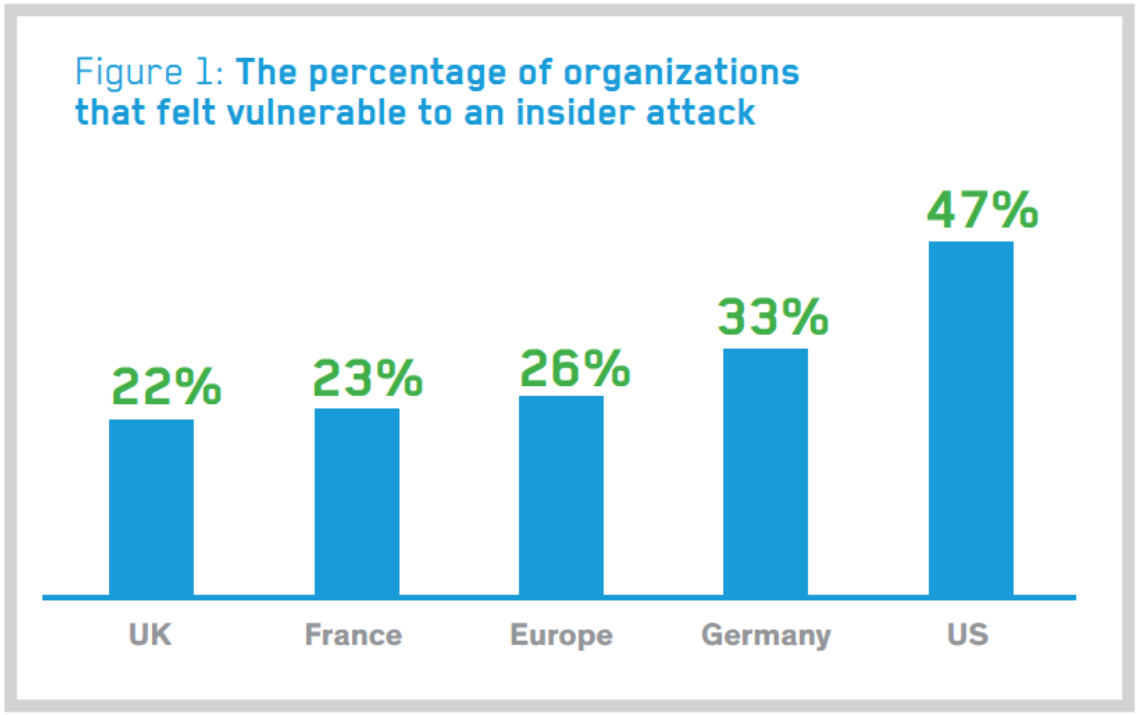
Figure 3: **The top 4 reasons why insider threats are more difficult to detect**

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]

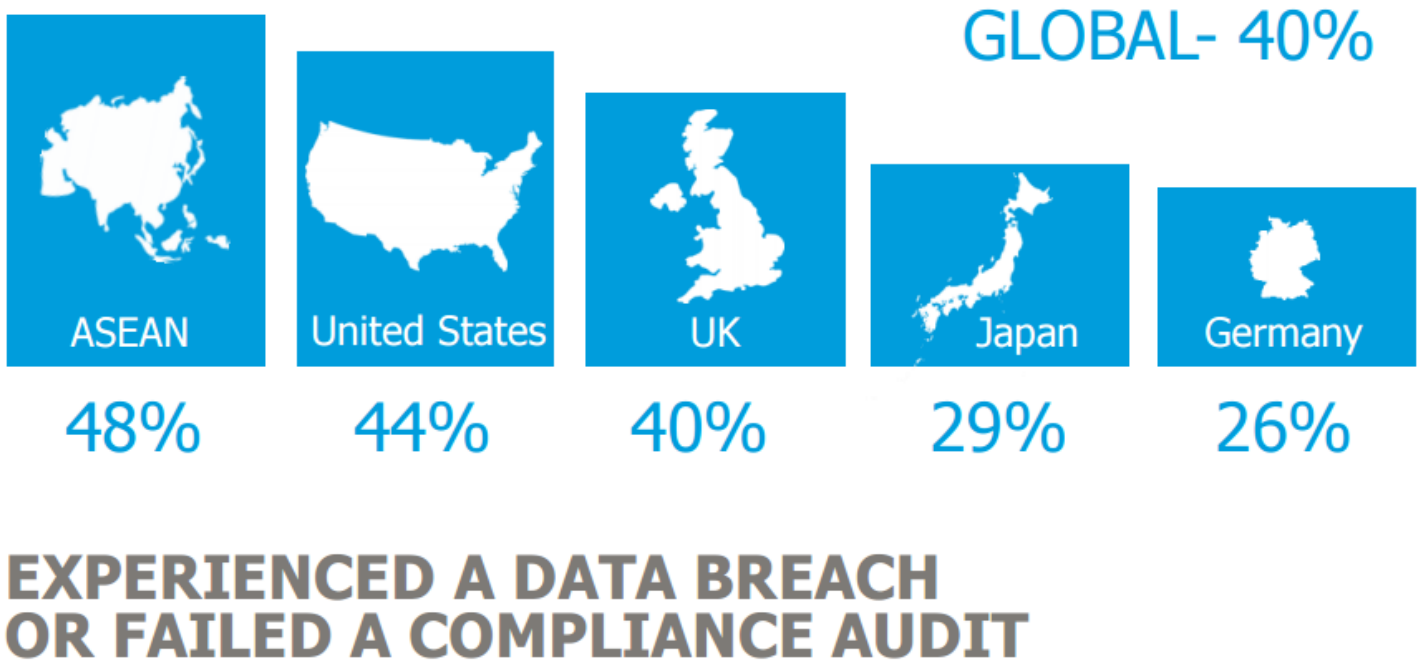
Iekšējo draudu ietekme

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]

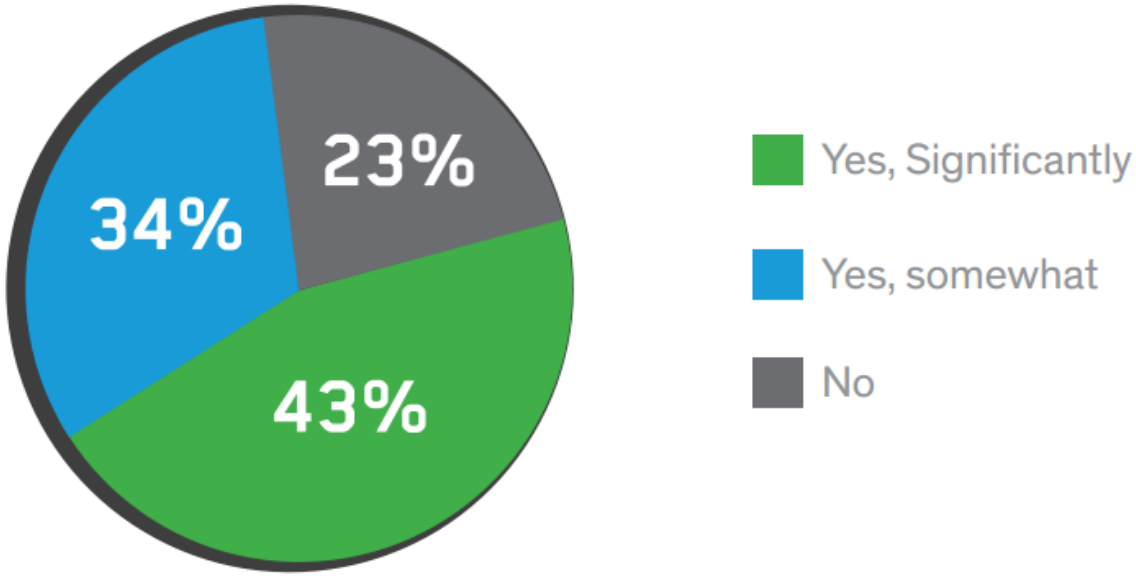
Iekšējo draudu ietekme



Avots [3]

Iekšējo draudu ietekme

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



Avots [2]

Iekšējo draudu ietekme

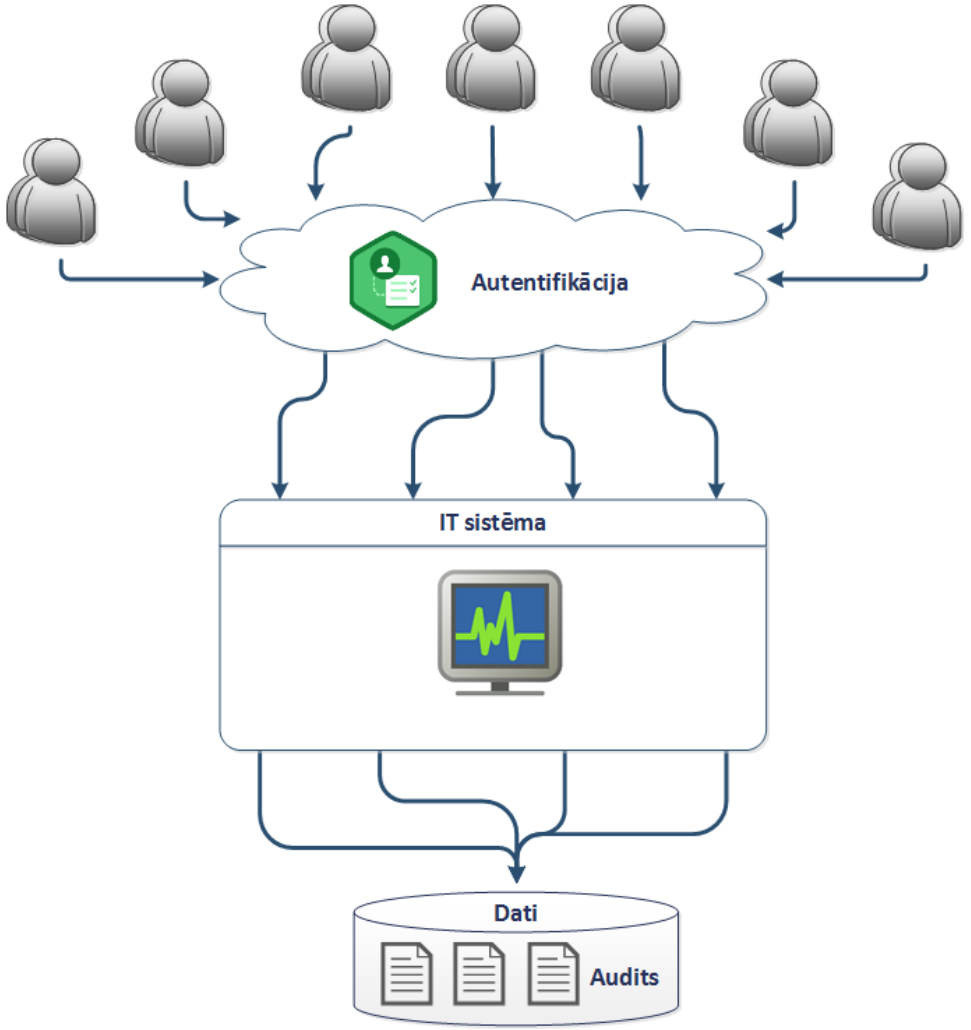
Avots [3]

Piedāvātais risinājums

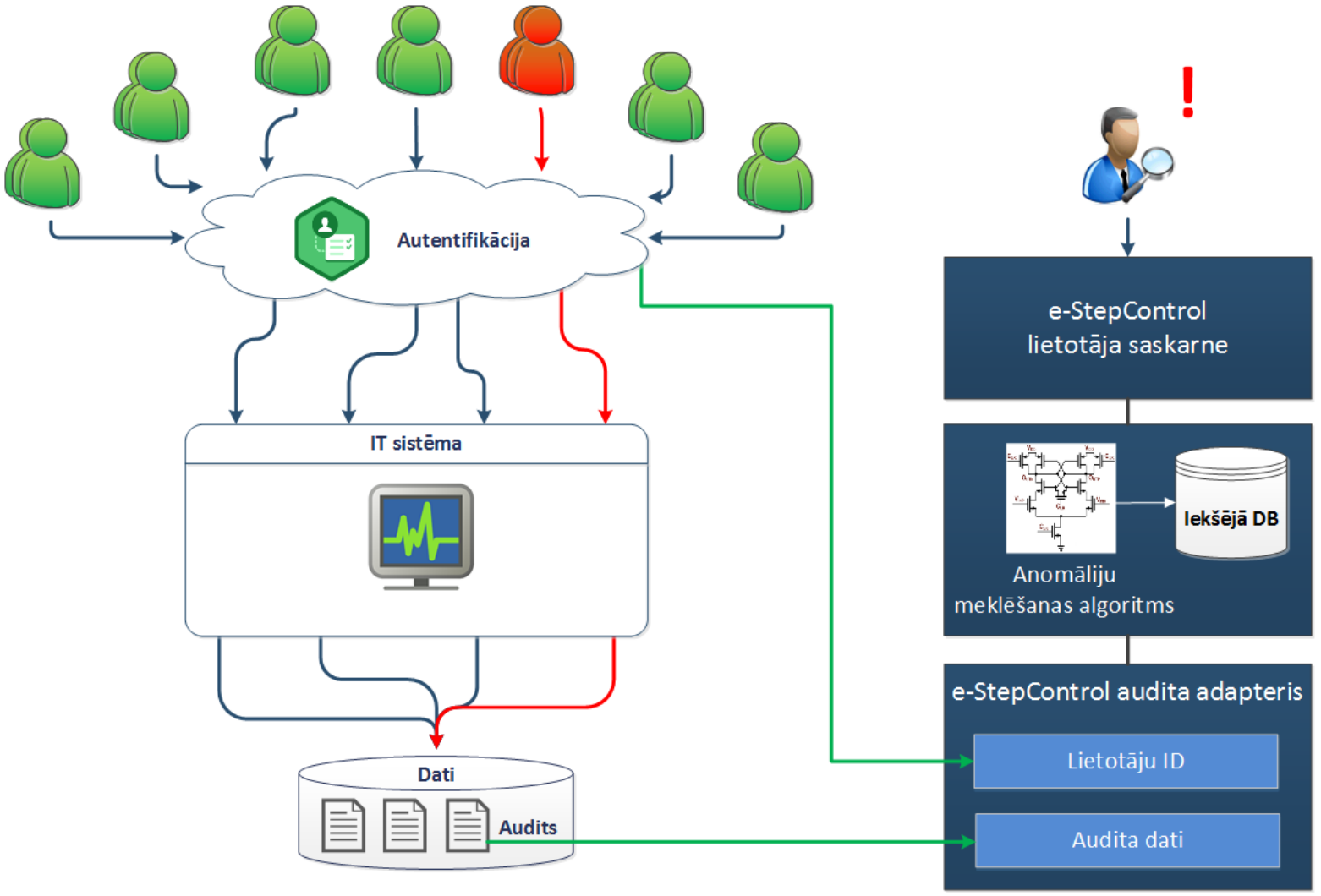
Risinājuma komponentes

- 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;

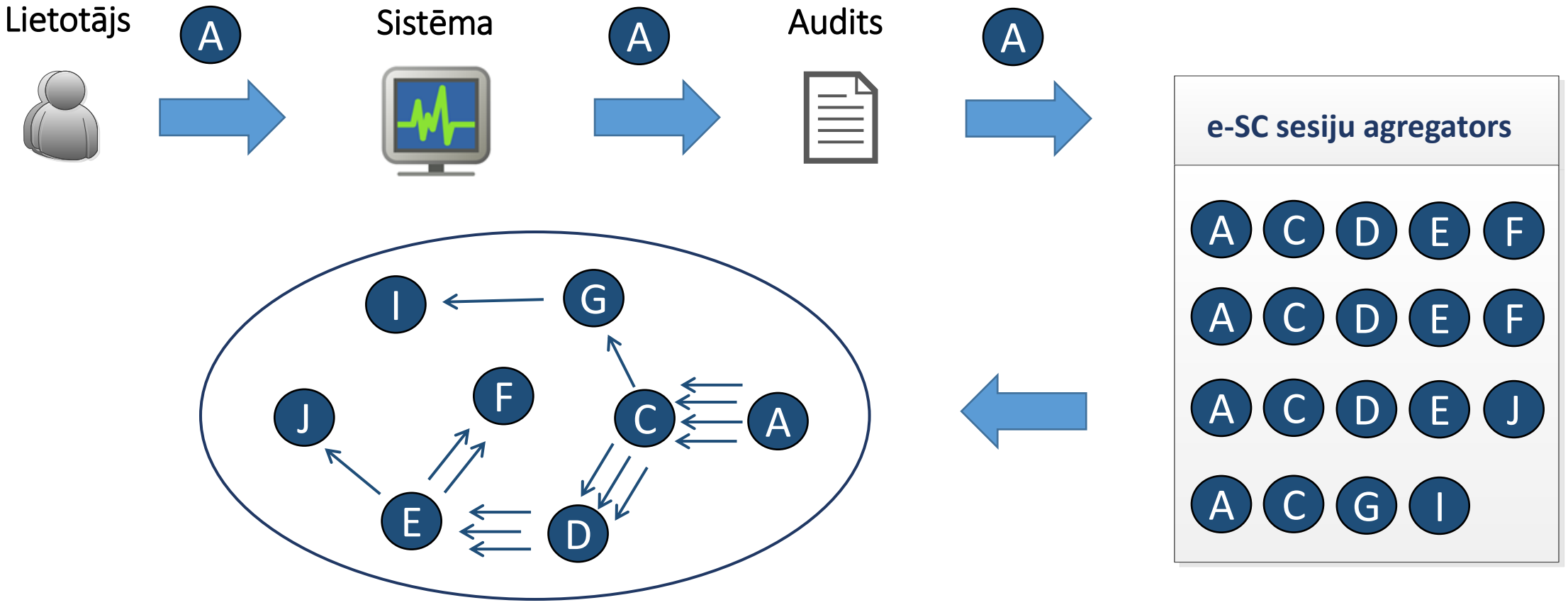
D – atlasīto ierakstu rezultāta apskatīšana;

E – ar konkrēto personu saistīto datu rediģēšana;

…

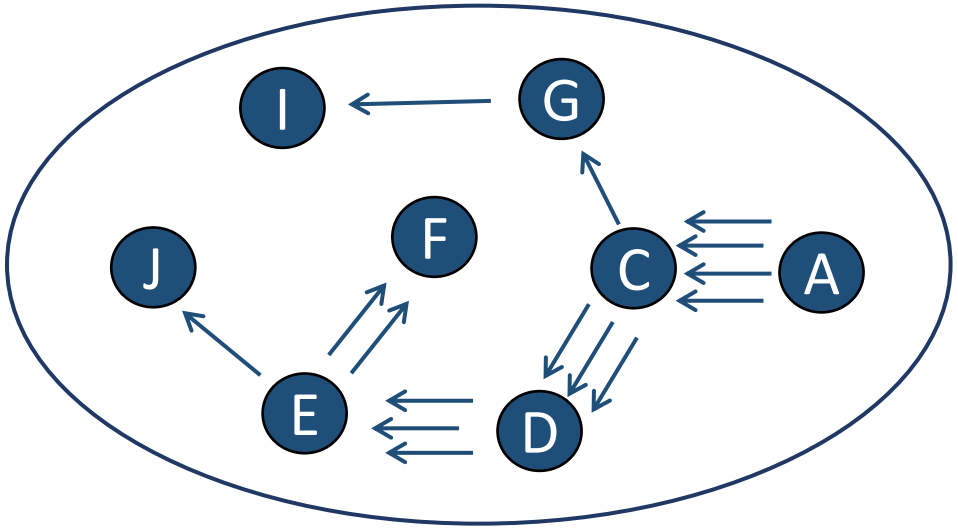
Z – izeja no sistēmas.

Pieeja: 1. solis – datu savākšana

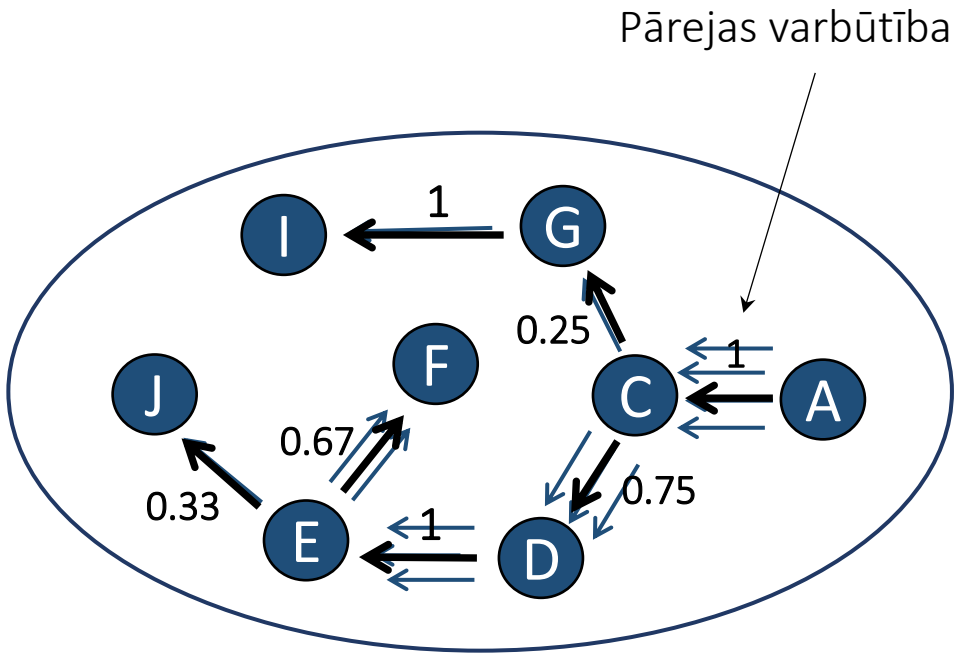


Lietotāja sesiju grafs

Pieeja: 2. solis – profilu izveidošana



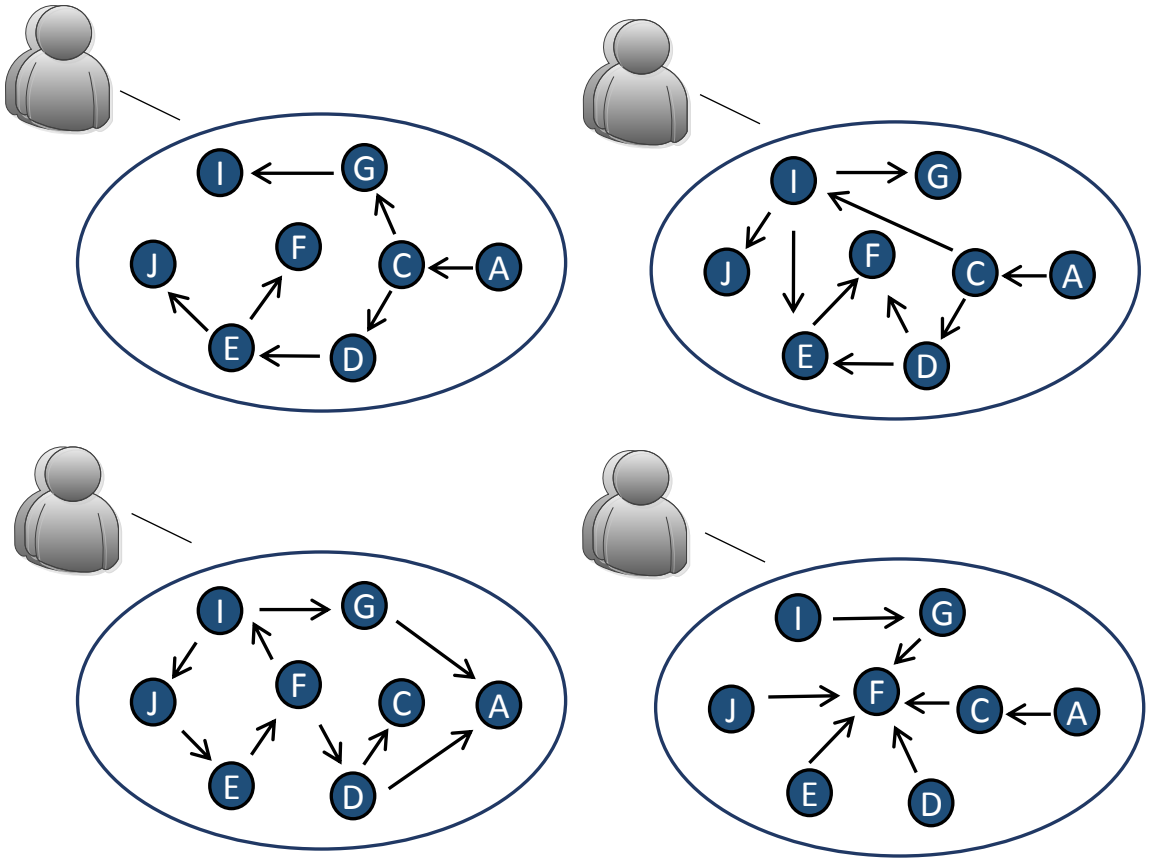
Lietotāja sesiju grafs



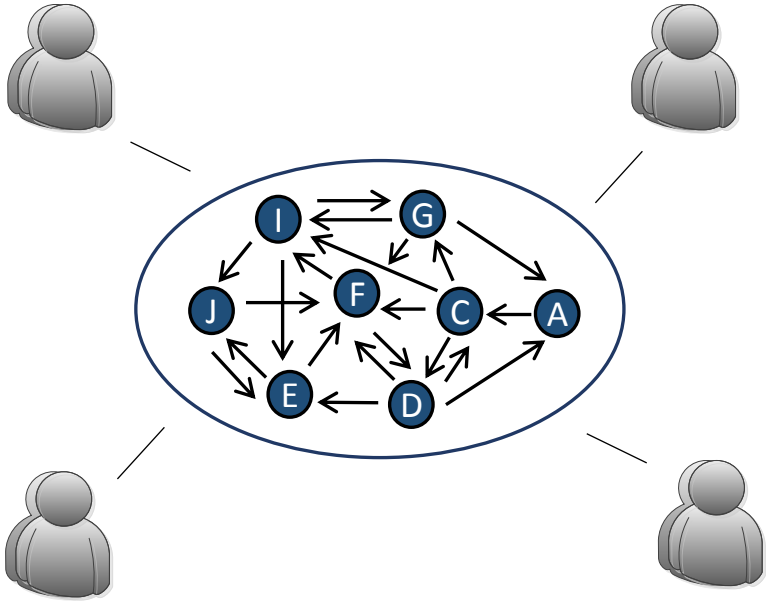
Lietotāja profila grafs

Pieeja: 2. solis – profilu izveidošana

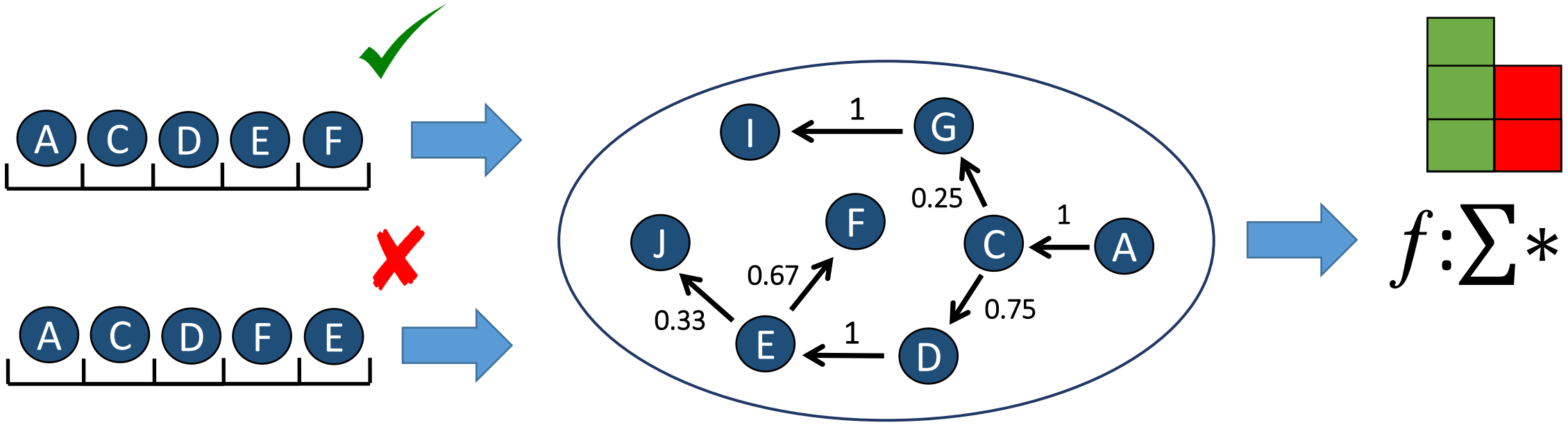
Individuālie lietotāju profili



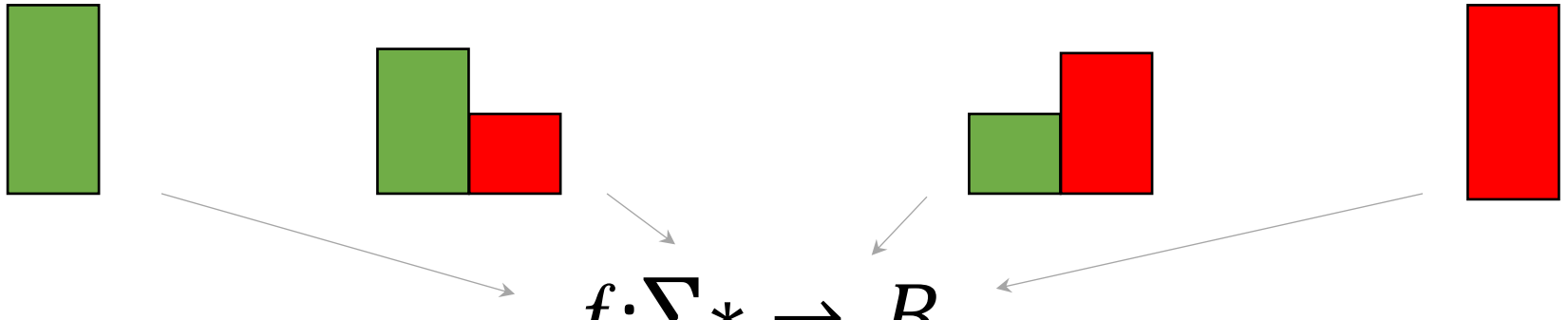
Kopējais grupas profils



Pieeja: 3. solis – monitorings

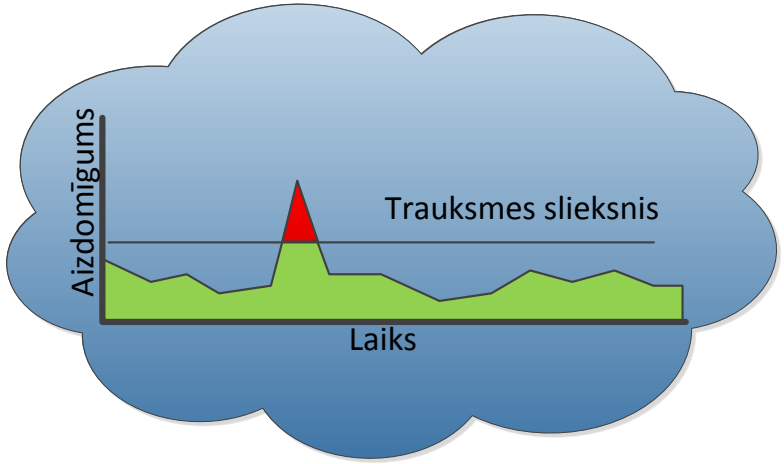


Pieeja: 3. solis – monitorings



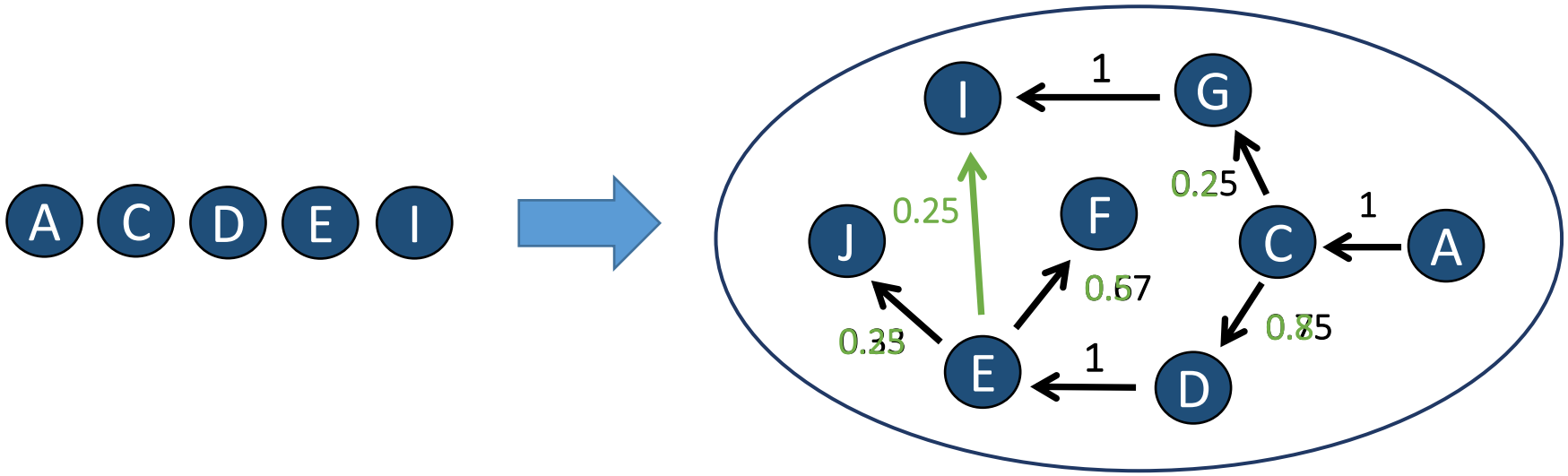
$$f: \sum * \rightarrow B$$

$$Aizdomīgums = \{\ 0 \quad \ldots \quad 0.33 \quad \ldots \quad 0.67 \quad \ldots \quad 1\ \}$$

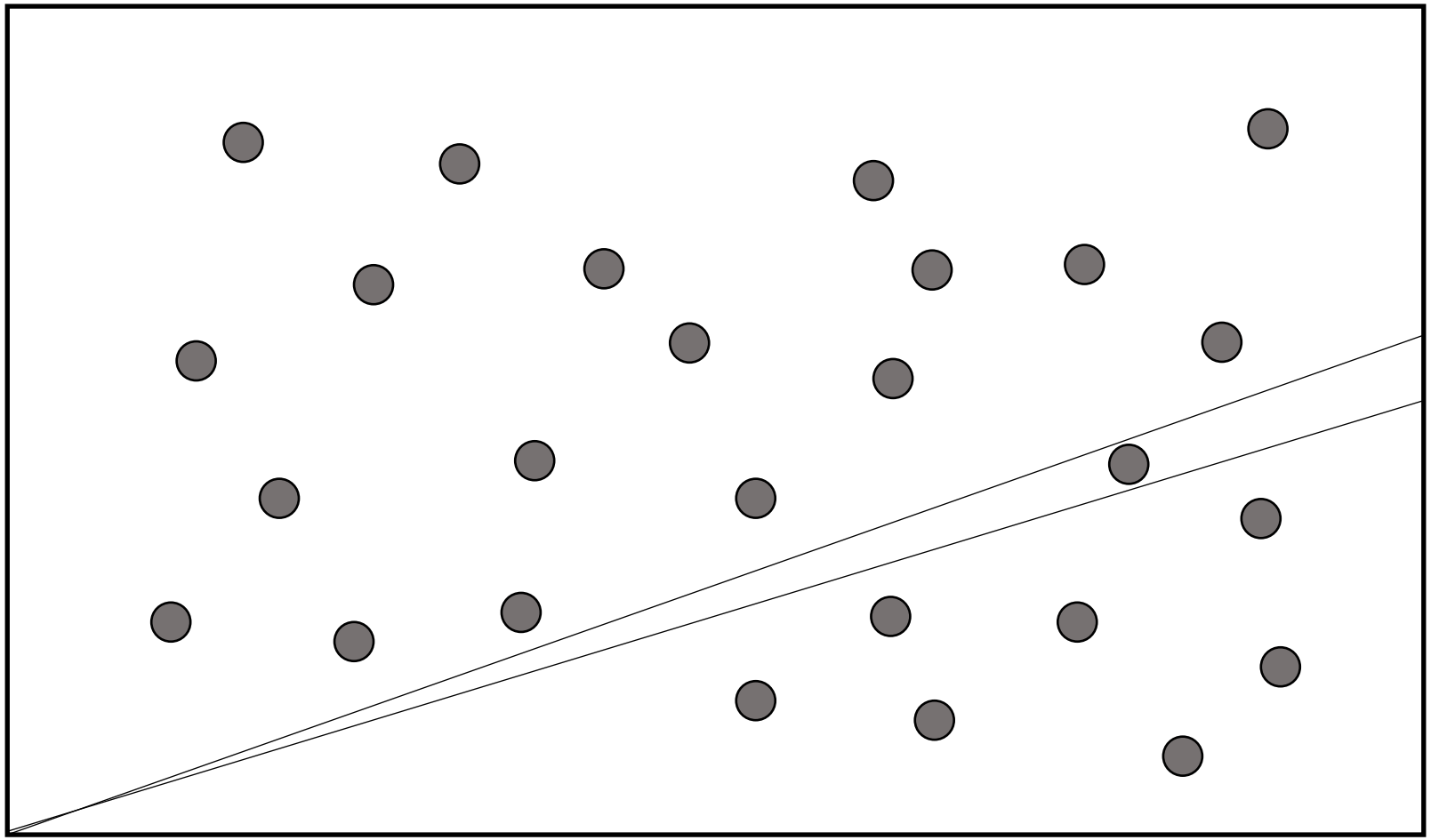


Pieeja: 3. solis – profila aktualizācija

$$Aizdomīgums = \{\ 0 \quad \dots \quad 0.33 \quad \dots \quad 0.67 \quad \dots \quad 1\ \}$$

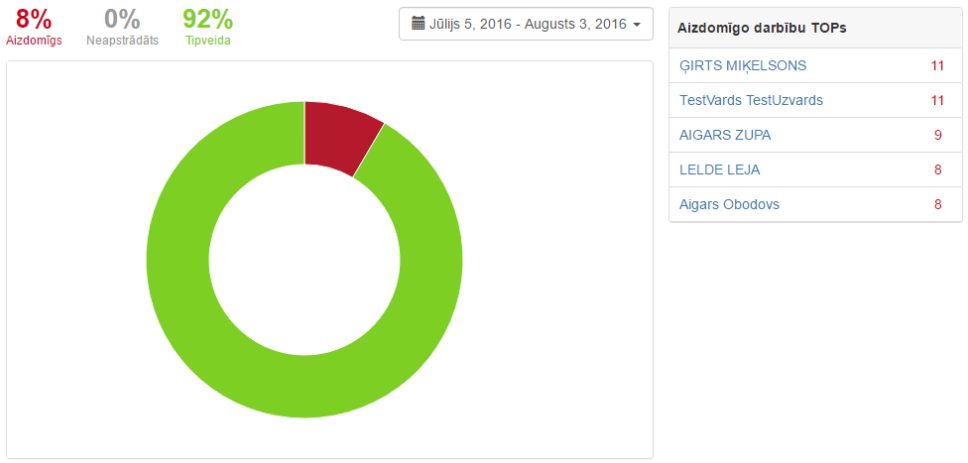


Pieeja: 3. solis – profila aktualizācija

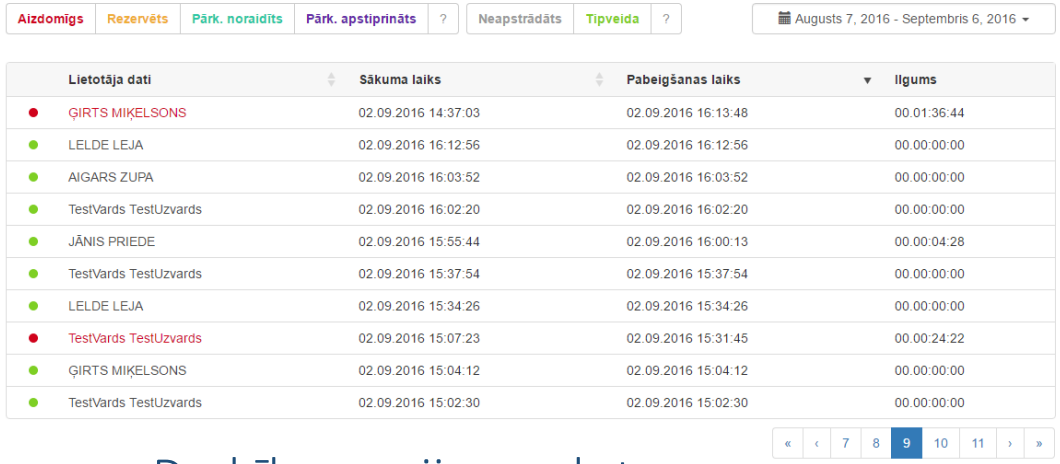


- Neizanalizētā datu kopa
- Klasifikācija ir pabeigta
- Sistēma ir apmācīta
- Pozitīvais scenārijs
- Negatīvais scenārijs
- Negatīvais scenārijs (?)
- Statusa precizējums
- Klasifikācijas korekcija

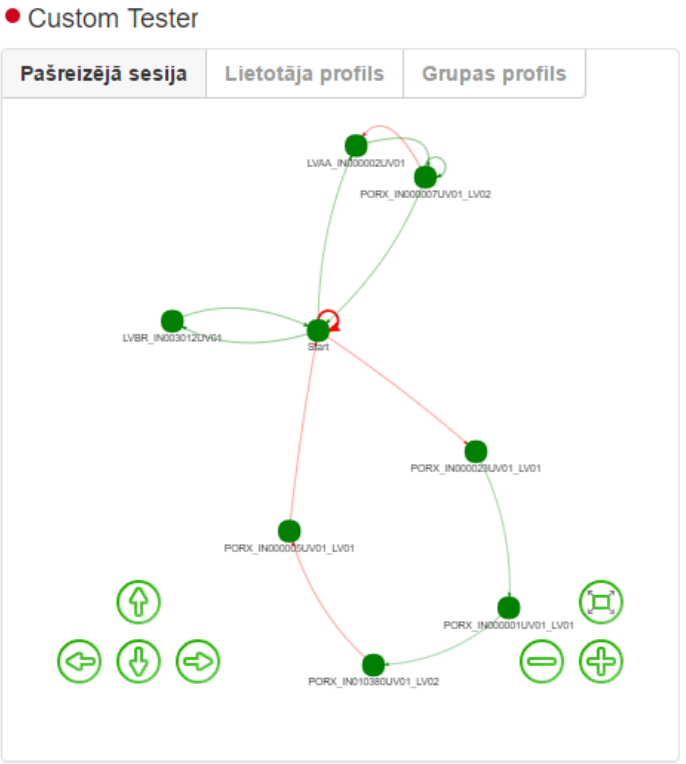
e-SC lietotāja saskarne



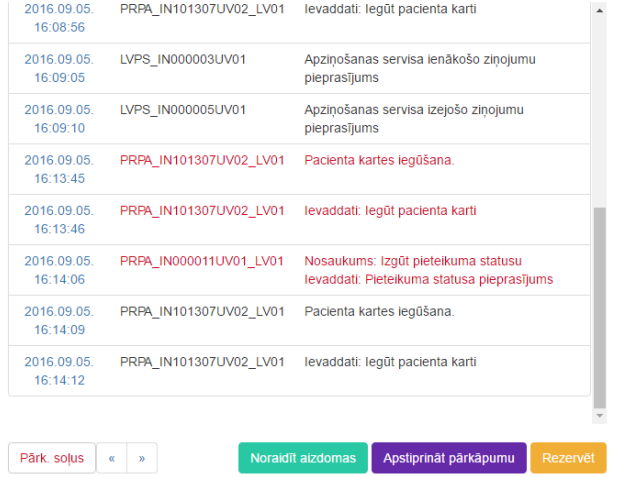
Statistika, aizdomīgo lietotāju “Top-5”



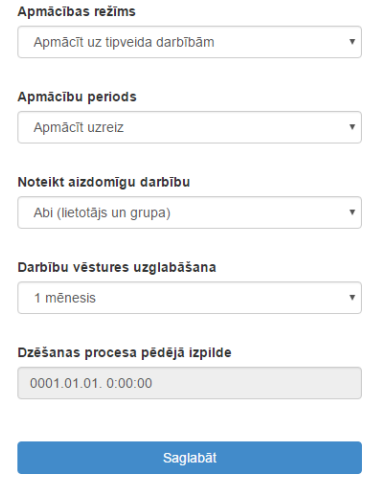
Darbības sesiju saraksts



Lietotāju profilu vizuālā analīze



Pārkāpumu soļu izpēte

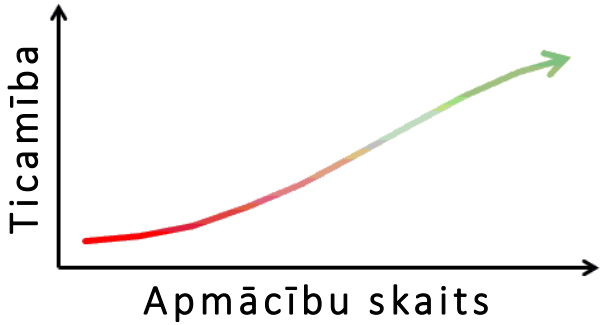


e-SC algoritma konfigurācija

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:

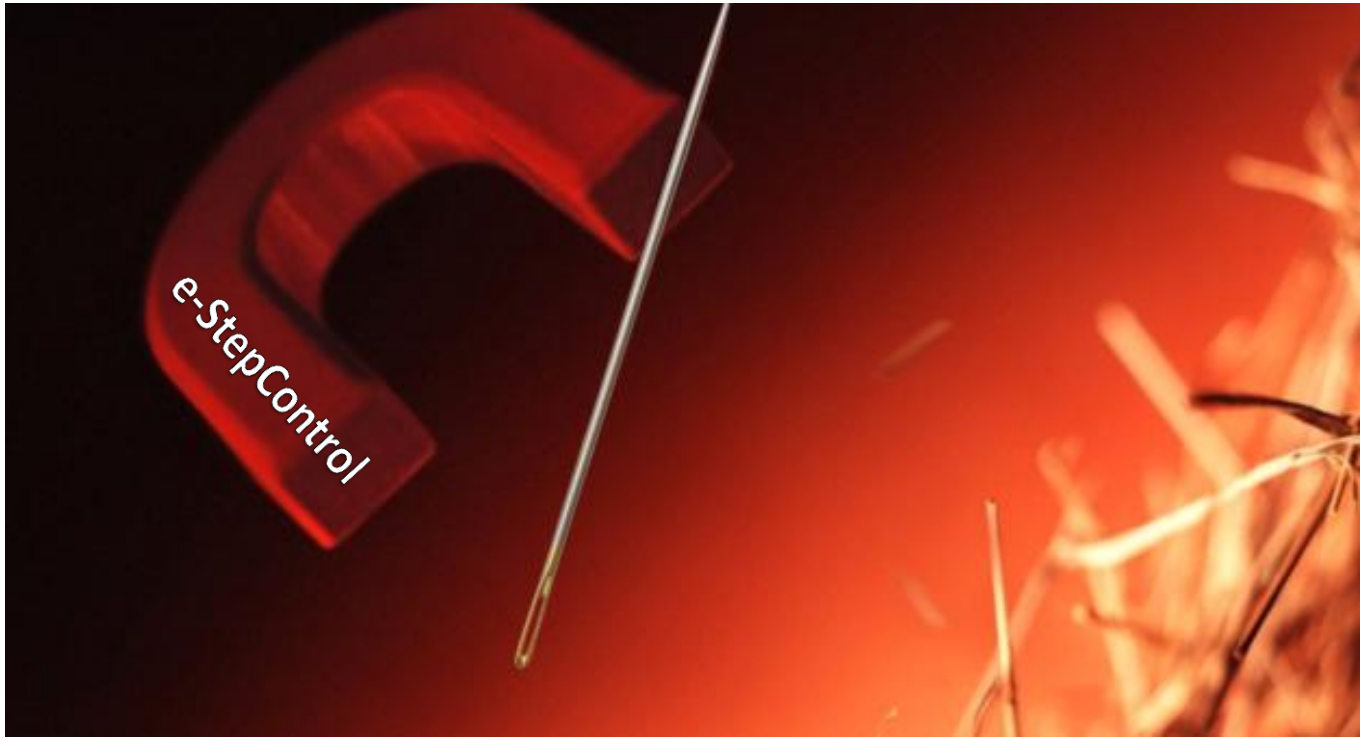


- Attīstot e-StepControl risinājumu, tiek veikti turpmākie pētījumi, lai būtu iespējams analizēt arī citus lietotāju raksturojumus:
  - ✓ IP adreses;
  - ✓ piekļuves laikus;
  - ✓ utt.

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!