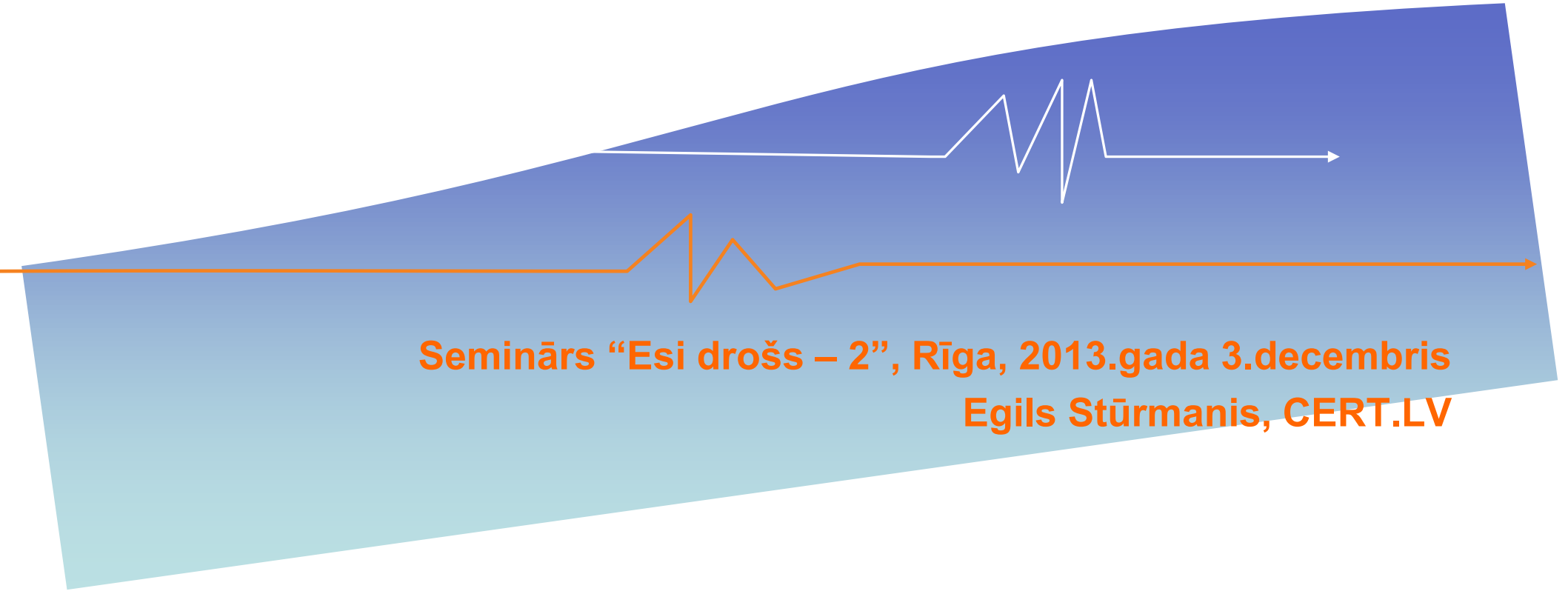
CERT.LV sadarbība ar valsts un pašvaldību institūcijām



Seminārs “Esi drošs – 2”, Rīga, 2013.gada 3.decembris

Egils Stūrmanis, CERT.LV

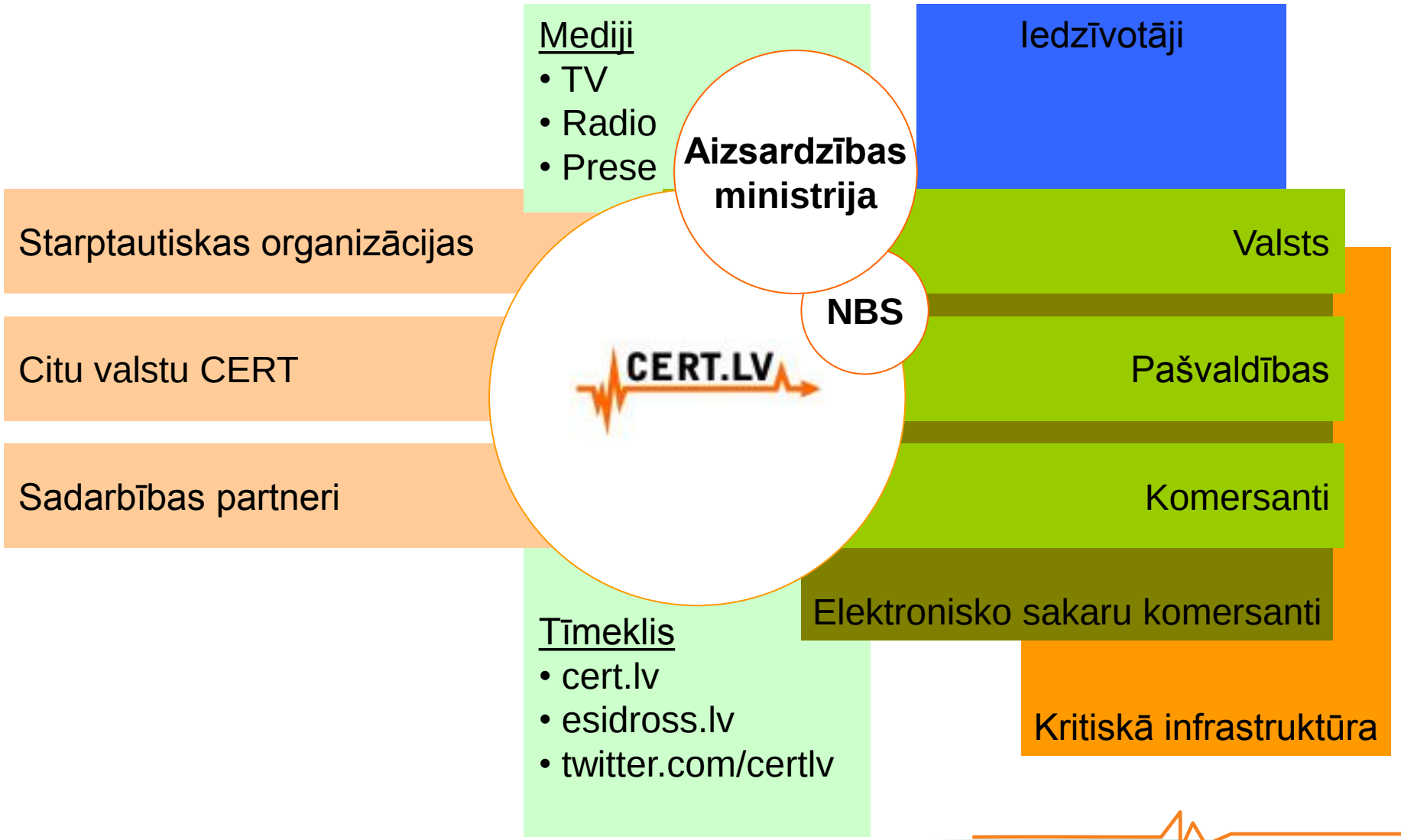
Saturs

- Informācijas tehnoloģiju drošības likums un saistītie MK noteikumi
- Sadarbības partneri
- Sadarbības principi
- Kopsavilkums

IT drošības likums un saistītie MK noteikumi

- IT drošības likums – 8.pants
  - Institūcijas vadītājs nosaka atbildīgo personu par IT drošības pārvaldību un par to informē CERT.LV
  - Atbildīgā persona
    - organizē IT drošības pārvaldību,
    - ne retāk kā reizi gadā veic IT drošības pārbaudes,
    - vismaz reizi gadā apmeklē CERT.LV rīkotos seminārus
    - ne retāk kā reizi gadā veic darbinieku apmācību
- MK not. Nr.100 – attiecas uz kritisko infrastruktūru
- MK not. Nr. 327 - attiecas ESK darbību

Sadarbības partneri



Informācijas apmaiņa (1)

Notikumu saraksts katru dienu no sensoriem

- Automātiski datubāzē – pamatā izmanto ESK (ISP)
- Automātiski csv formāta fails uz e-pastu (testa režīmā)
- Incidentu ziņojumi manuāli apstrādāti uz e-pastu

Ziņojumi uz e-pastu no incidentu *Tracking* sistēmas

- Incidentu ziņojumi manuāli apstrādāti un nosūtīti uz e-pastu

Brīdinājumi e-pasti

- kalendārie
- uz notikumiem balstīti

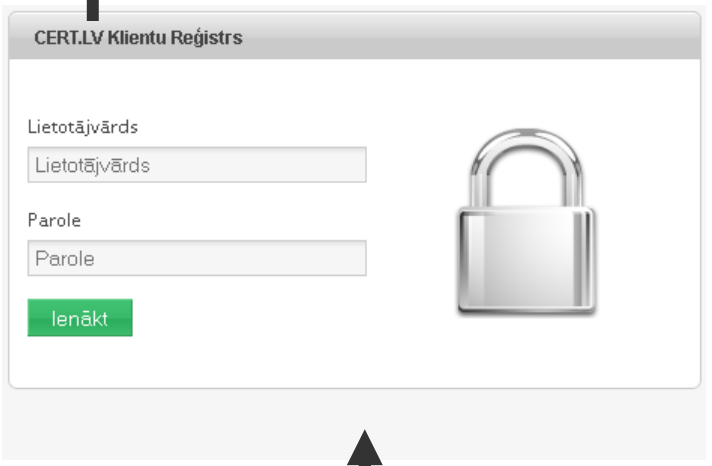
Dokumentu paraugi CERT.LV tīmekļa vietnē

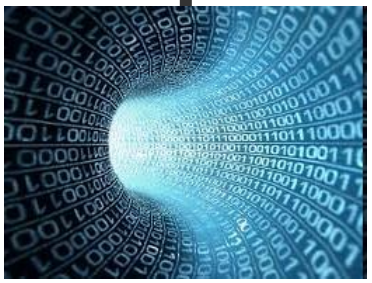
- IDIP
- IT drošības noteikumu paraugs
- Rīcības plāna paraugs

Informācijas apmaiņa (2)

CERT.LV darbinieka sūtīts ziņojums vai zvans

CERT.LV robota sūtīts ziņojums ESK SQL formātā





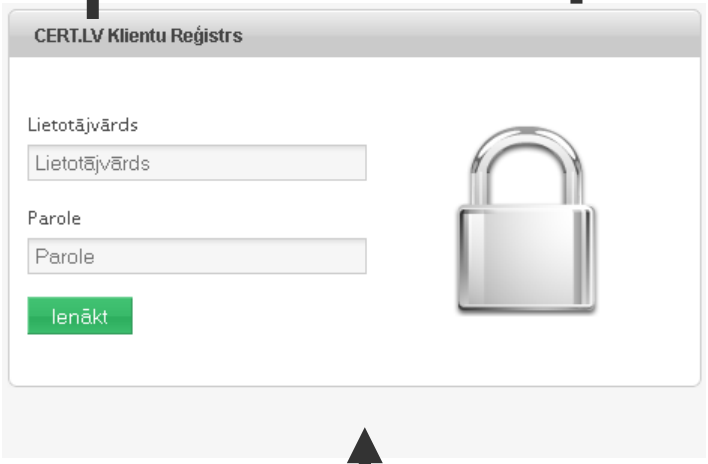
Sadarbības partneru sensori

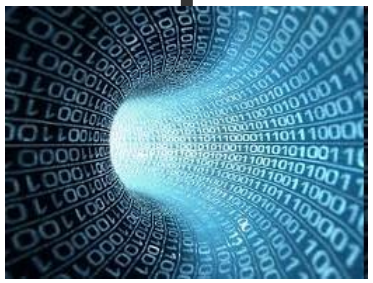
Informācijas apmaiņa (3)

CERT.LV darbinieka sūtīts ziņojums vai zvans

CERT.LV robota sūtīts ziņojums ESK SQL formātā

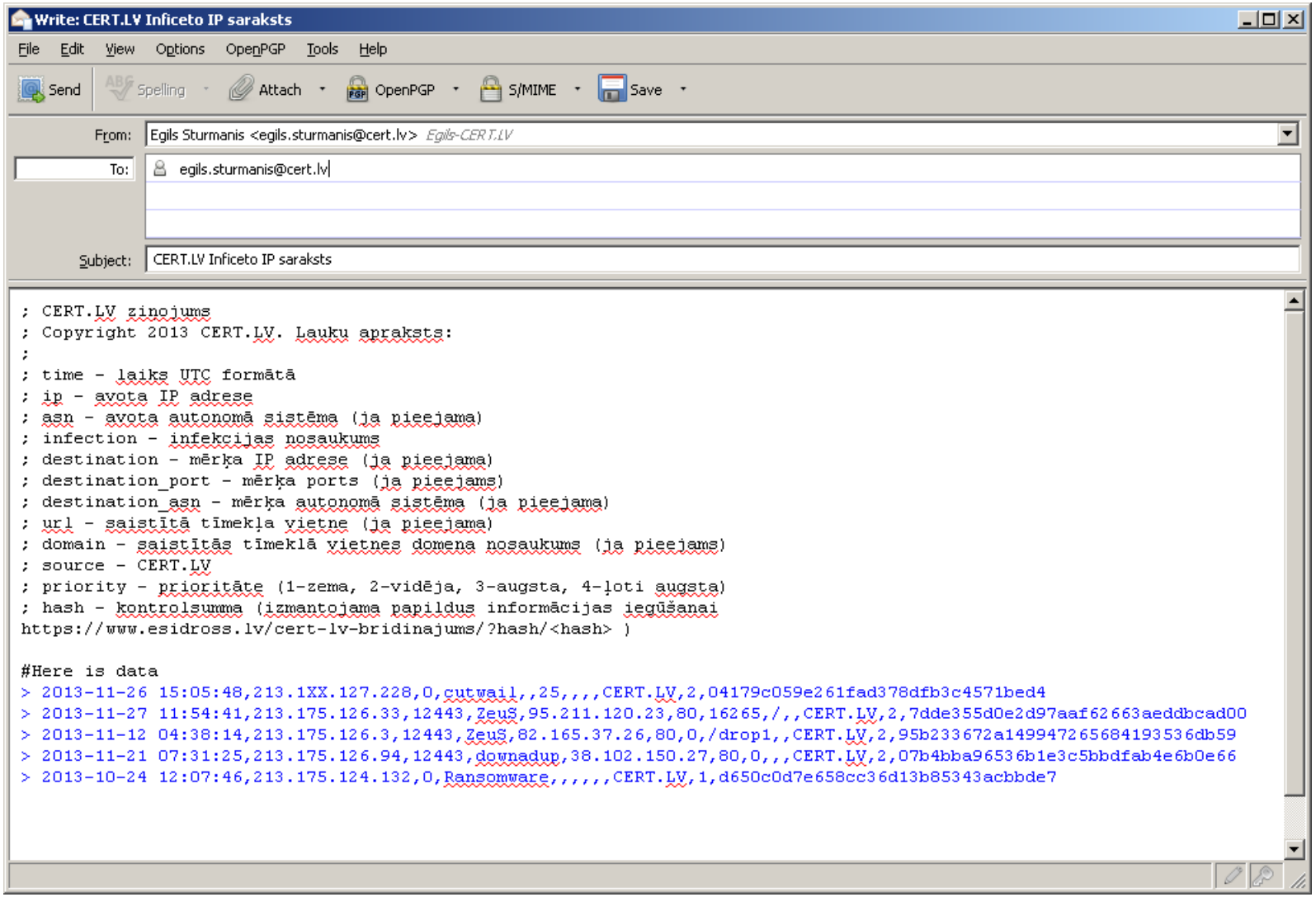
CERT.LV robota sūtīts ziņojums csv formātā





Sadarbības partneru sensori

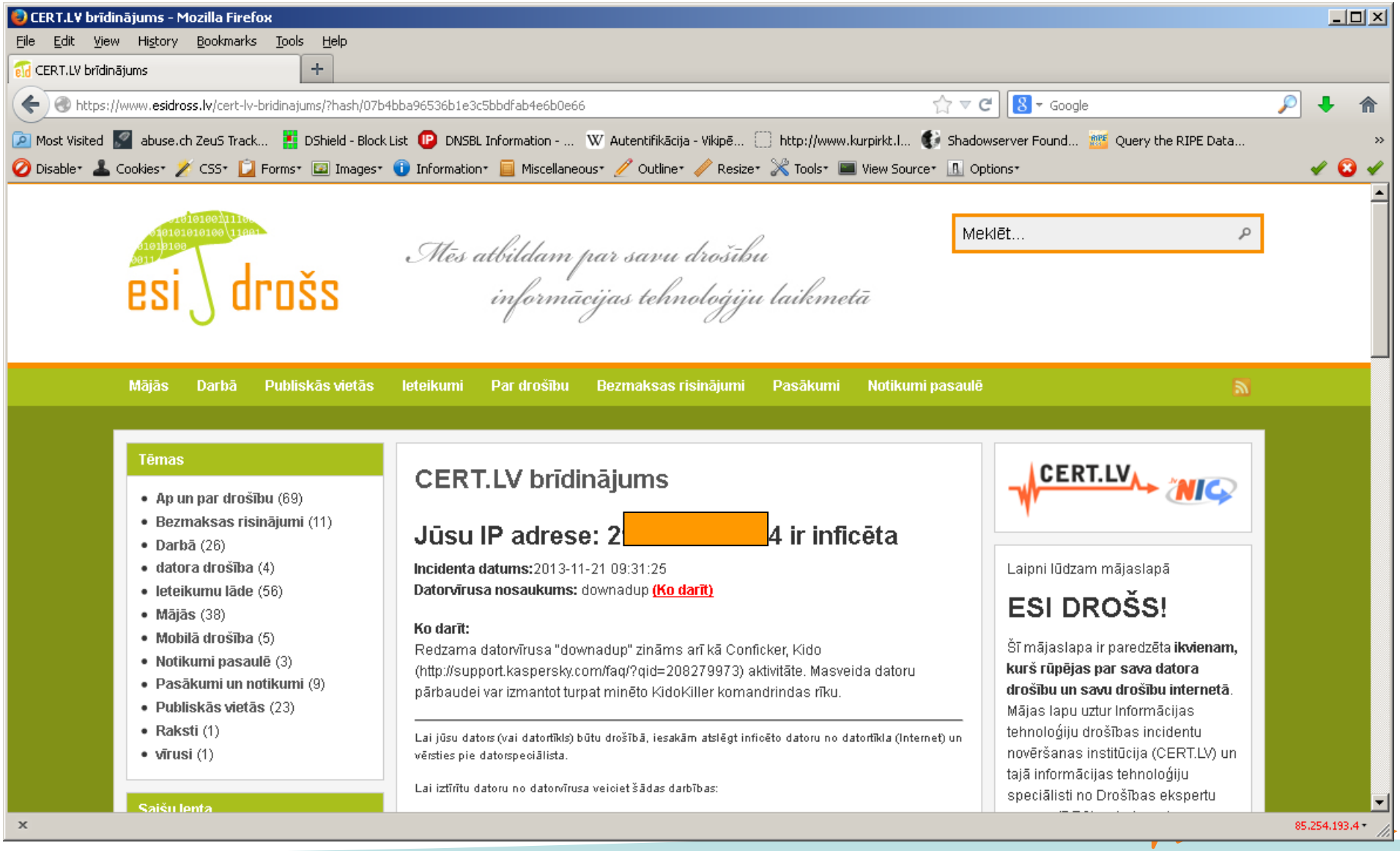
CERT.LV ziņojums CSV formātā



Ziņojuma formāta skaidrojums

; time - laiks UTC formātā
; ip - avota IP adrese
; asn - avota autonomā sistēma (ja pieejama)
; infection - infekcijas nosaukums
; destination - mērķa IP adrese (ja pieejama)
; destination_port - mērķa ports (ja pieejams)
; destination_asn - mērķa autonomā sistēma (ja pieejama)
; url - saistītā tīmekļa vietne (ja pieejama)
; domain - saistītās tīmekļa vietnes domēna nosaukums (ja pieejams)
; source - CERT.LV
; priority - prioritāte (1-zema, 2-vidēja, 3-augsta, 4-ļoti augsta)
; hash - kontrolsumma (izmantojama papildus informācijas iegūšanai https://www.esidross.lv/cert-lv-bridinajums/?hash/<hash>)

Hash kontrolsummas izmantošana esidross.lv

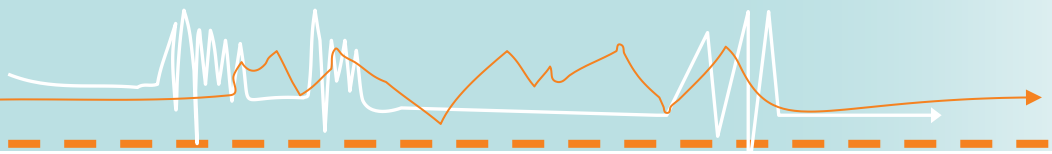


Kas nepieciešams

- Iestādēm:
  - Atbildīgā persona (elektroniskais pasts)
  - IP adrešu lauks
  - labā griba saņemto informāciju, apstrādāt to un sadarboties ar CERT.LV
- CERT.LV: izsūtīt e-pastu ar lūgumu
  - sniegt informāciju par savā atbildībā esošajiem resursiem (ja informācijas nav)
  - aktualizēt informāciju par savā atbildībā esošajiem resursiem (ja informācija ir)
    - aktualizācija paredzēta reizi gadā

Kopsavilkums

- Ziņojumi CSV formātā no 2014.01.01 tiks izsūtīti visu iestāžu atbildīgajiem par IT drošību, kuru e-pasti un IP adrešu laiku ir zināmi
- CERT.LV darbinieku apstrādātie ziņojumi no *Tracking* sistēmas tiks izsūtīti manuāli un parakstīti ar CERT GPG atslēgu
- Ziņojumu apstrādes un izsūtīšanas automatizācija
  - nekavējoši nosūta informāciju
  - nepieļauj kļūdas informācijas apmaiņā
  - portālā esidross,lv atbalsts/palīdzība katram ziņojuma notikumam 24x7
  - atslogo CERT.LV cilvēkresursus
  - strādā arī brīvdienās un svētku dienās



CERT.LV

Paldies par uzmanību!

http://www.cert.lv

cert@cert.lv

egils.sturmanis@cert.lv