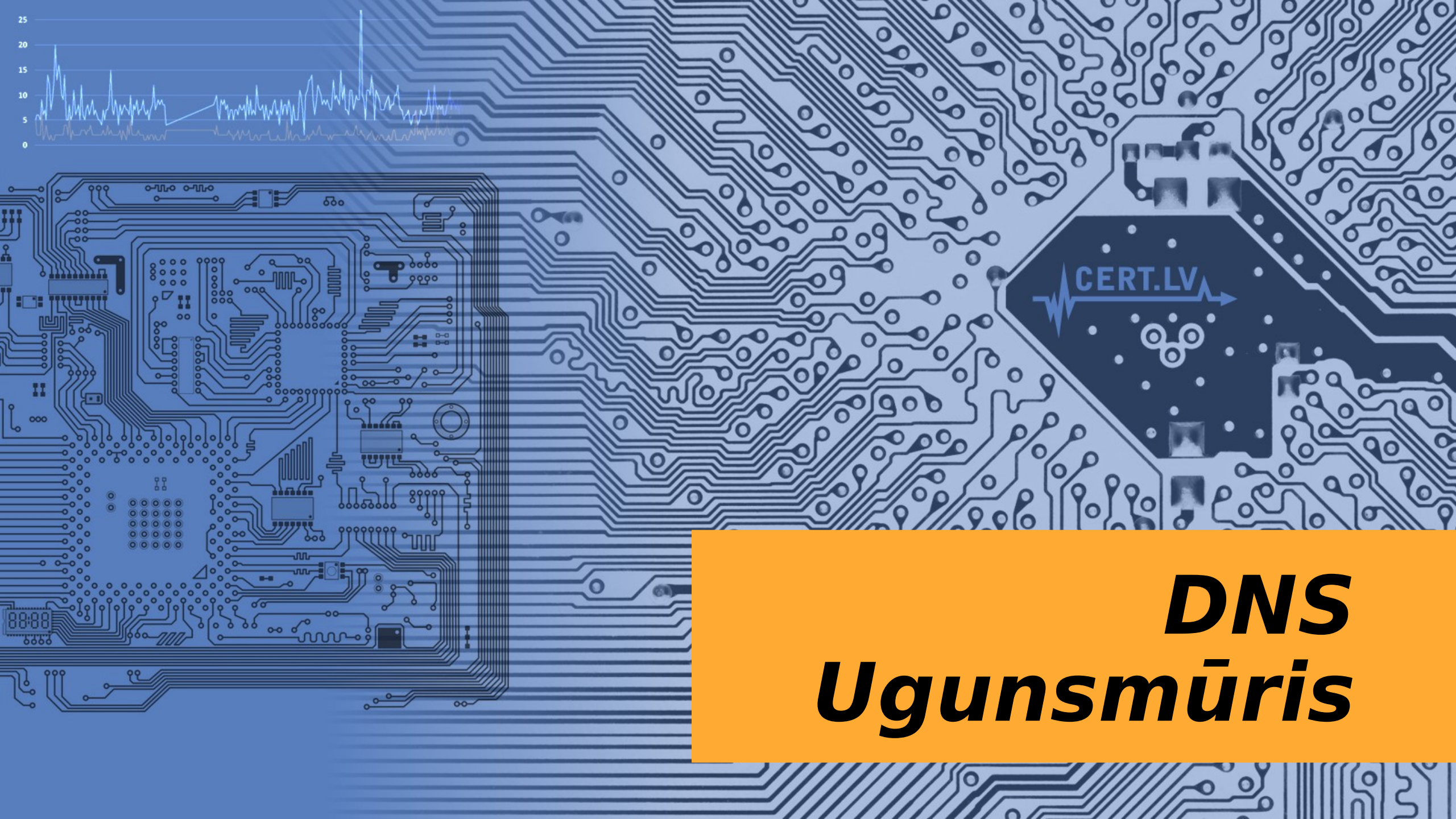


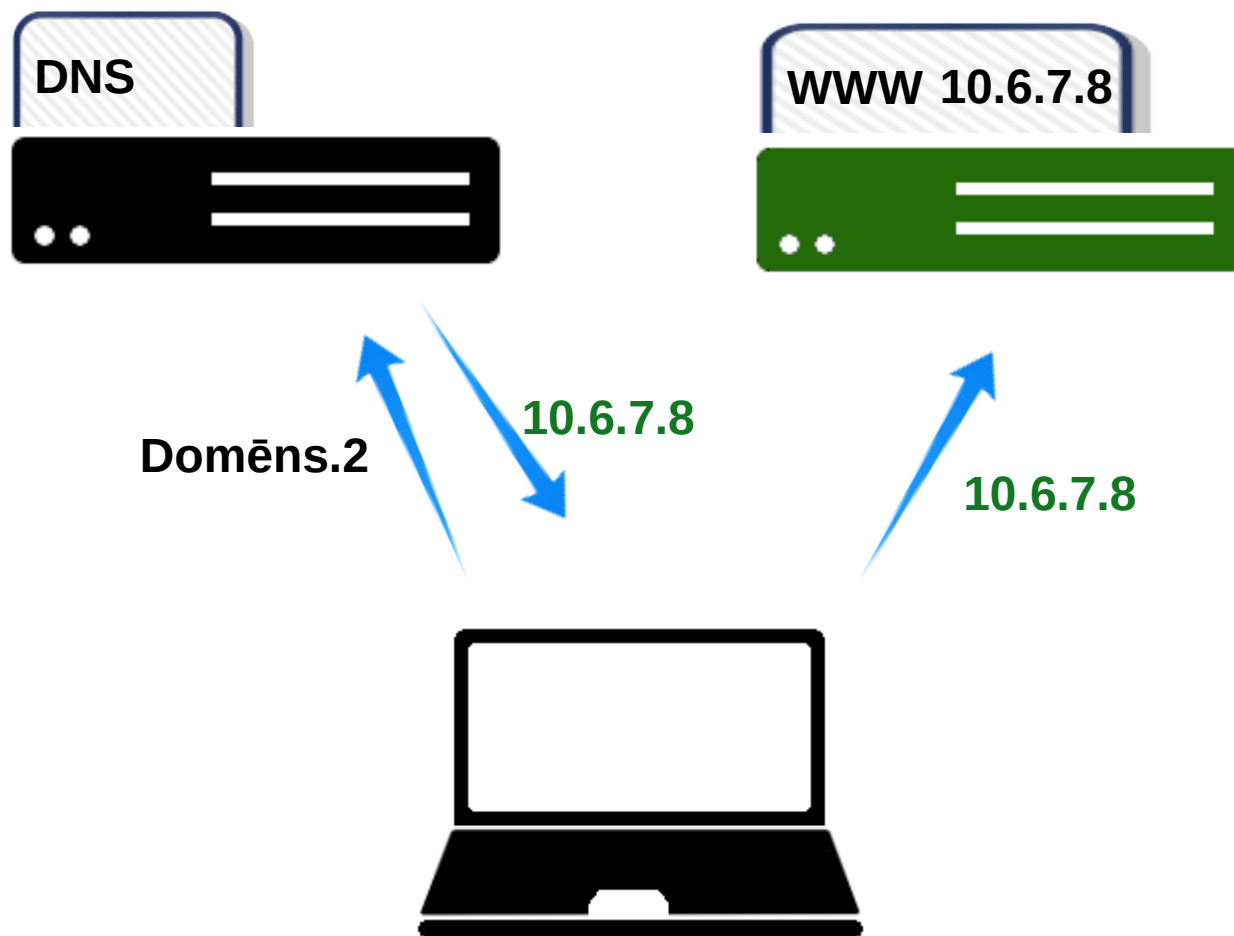
Apkopoījums par CERT.LV piedāvātajiem risinājumiem

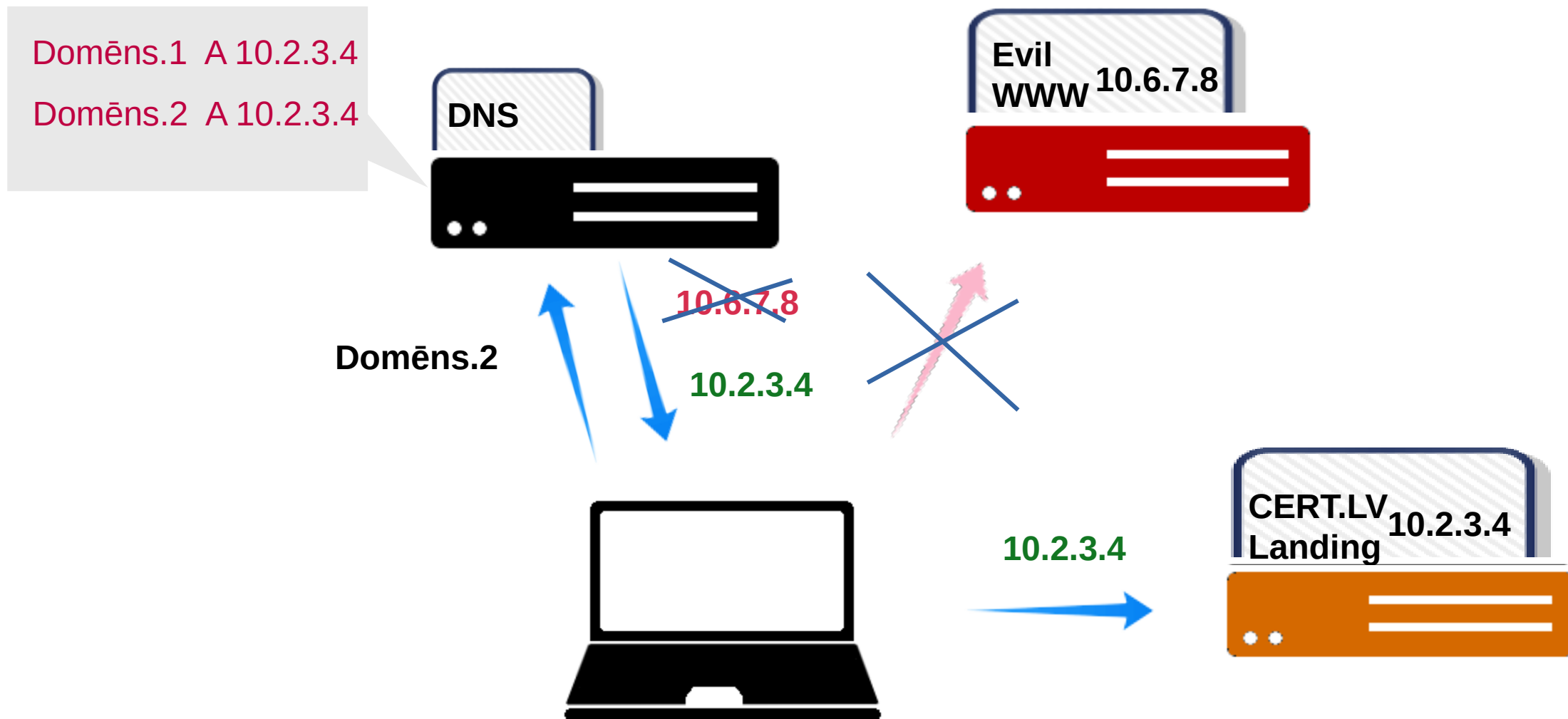


DNS Ugunsbūris

Kas tas ir?

DNS Ugunsmūris ir DNS (Domain Name System) serviss ar iespējamu RPZ (Response policy zone) tehnoloģiju





leguvumi...

- Aizsardzība no aktuālajām kampaņām Latvijā
- Izmantojams visā Latvijas teritorijā
- CERT.LV iesaiste





Svarīgs ziņojums!

Šodien mēs pārbaudām SEPA tūlītējo sistēmu.
Ja pierakstāties savā tiešsaistes kontā, pieņemiet mūsu simulācijas pārskaitījumu uz IBAN NL ** BUNQ **. SEPA tūlīt visiem klientiem ir jāpiekrīt šim testam.
Uzmanību! Šī nodošana ir tikai simulācija, jūsu nauda ir droša.

Mēs vēlreiz paziņojam, ka mēs esam tikai simulācija, kuru mēs neņemam no jūsu konta.
Paldies par sapratni.

Pieslēgties

1 Lietotāja kods 2 Parole

Lūdzu, ievadiet lietotāja kodu

Smart-ID



- Drošība
- Ne...
→ un...
→ nep...
→ inte...
→ līdz...
- Dro...
→ Kā...
→ Ne...
- Node...
- Inter...
- Pies...
- Val...
→ Mo...
→ Inte...
→ Infotelpa
- Ceļvedis
- Internetbankas ceļvedis
→ Darba uzsākšana internetbankā
→ Multivalūtu konts



trešd. 2019. gada .27.02 16:06

SEB banka <info84357@amexx.com>

You have 1 new message online

To

Note: This message has been scanned for viruses and dangerous content!

Dear customer ,

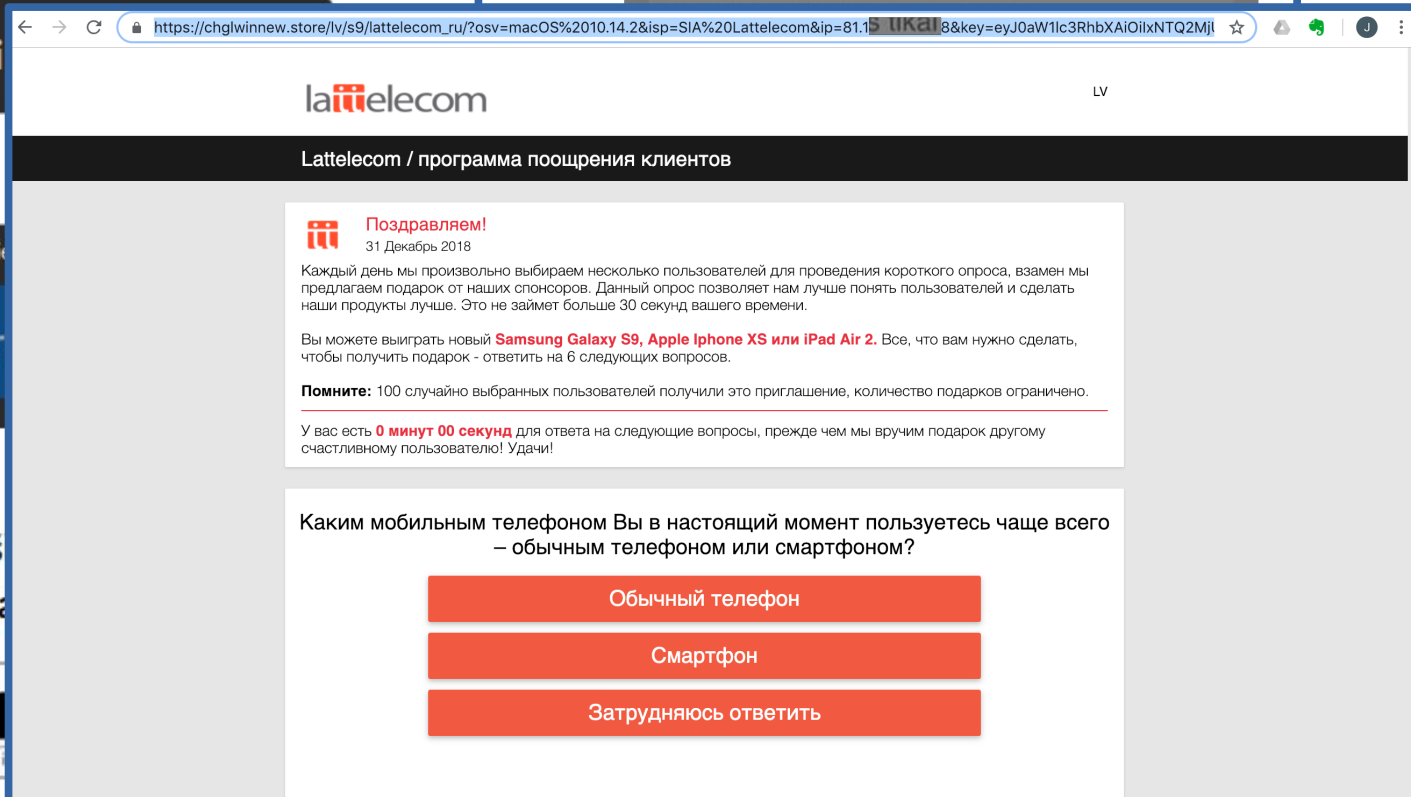
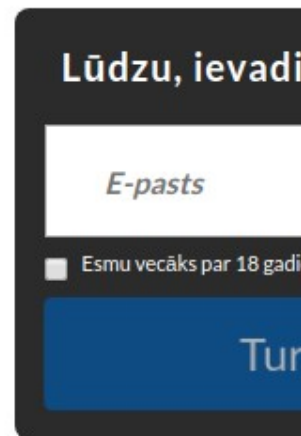
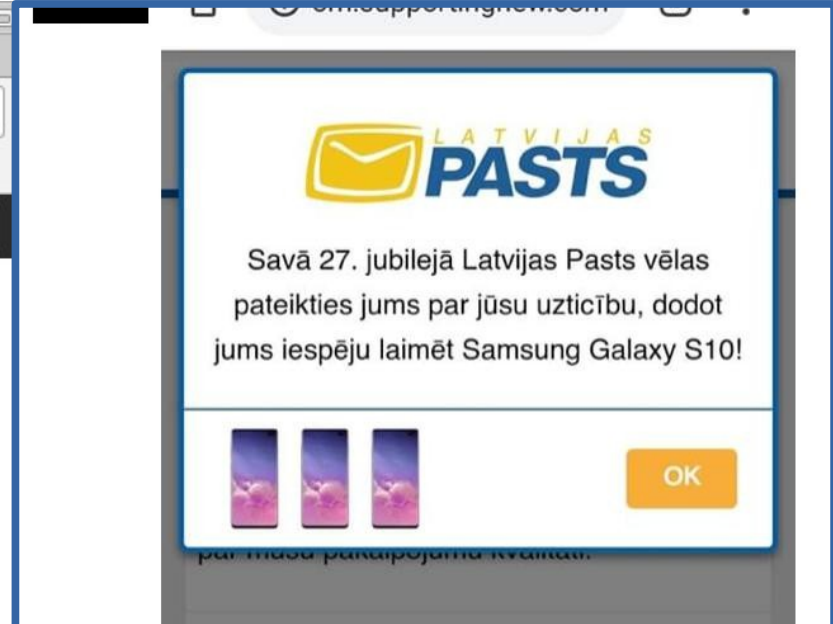
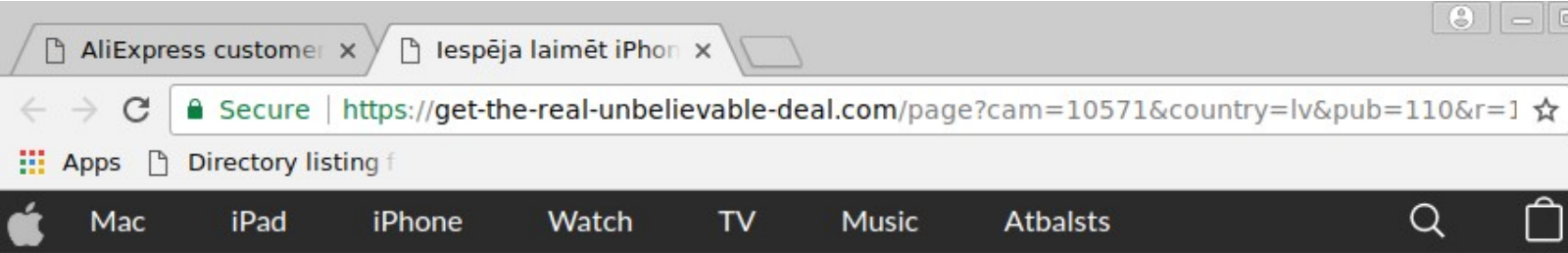
You have 1 new message online.

[Click here to read the message.](#)

This message is sent automatically, please do not reply.

SEB banka 2019





Log in to Continue Tracking your Package



Sign In With Your Correct Email and Password To Review Package Information

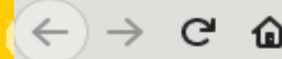
(*) Denotes required field.

* Email Address :

* Password :

Copyright Notice © 1999-2017 DHL WorldWide Delivery. All rights reserved.

Adobe PDF Plugin Install for all



<https://adobeupdt.net/En-US/reader/download>



Adobe PDF Plugin



Initializing

1. To proceed, open

Markets Invest

<https://markets-invest.com>



ABOUT US

BROKERAGE SERVICES

LICENSING

REGISTRATION

Trading conditions

Indices, Majors, Commodities, ETF, CFD,
Crypto currencies

START EARNING

Send us a message

Business Messenger

Please leave your message in the fo
and we will reply by e-mail

Закрепительный платёж

Онлайн оплата

payonline

Сумма списания в рублях: 193,00 руб

Verified by
VISA

Принимаются к оплате:



КРЕДИТНАЯ/ДЕБЕТОВАЯ КАРТА

НОМЕР КАРТЫ

XXXX XXXX XXXX XXXX

СРОК
ДЕЙСТВИЯ

МЕСЯЦ

ГОД

01

2019

Люкс Банк

ОПЛАТИТЬ

CVC CODE

XXX 123

Для совершения оплаты введите код CVC2/CVV2. Он
расположен на задней стороне карты

Kā pieslēgt?

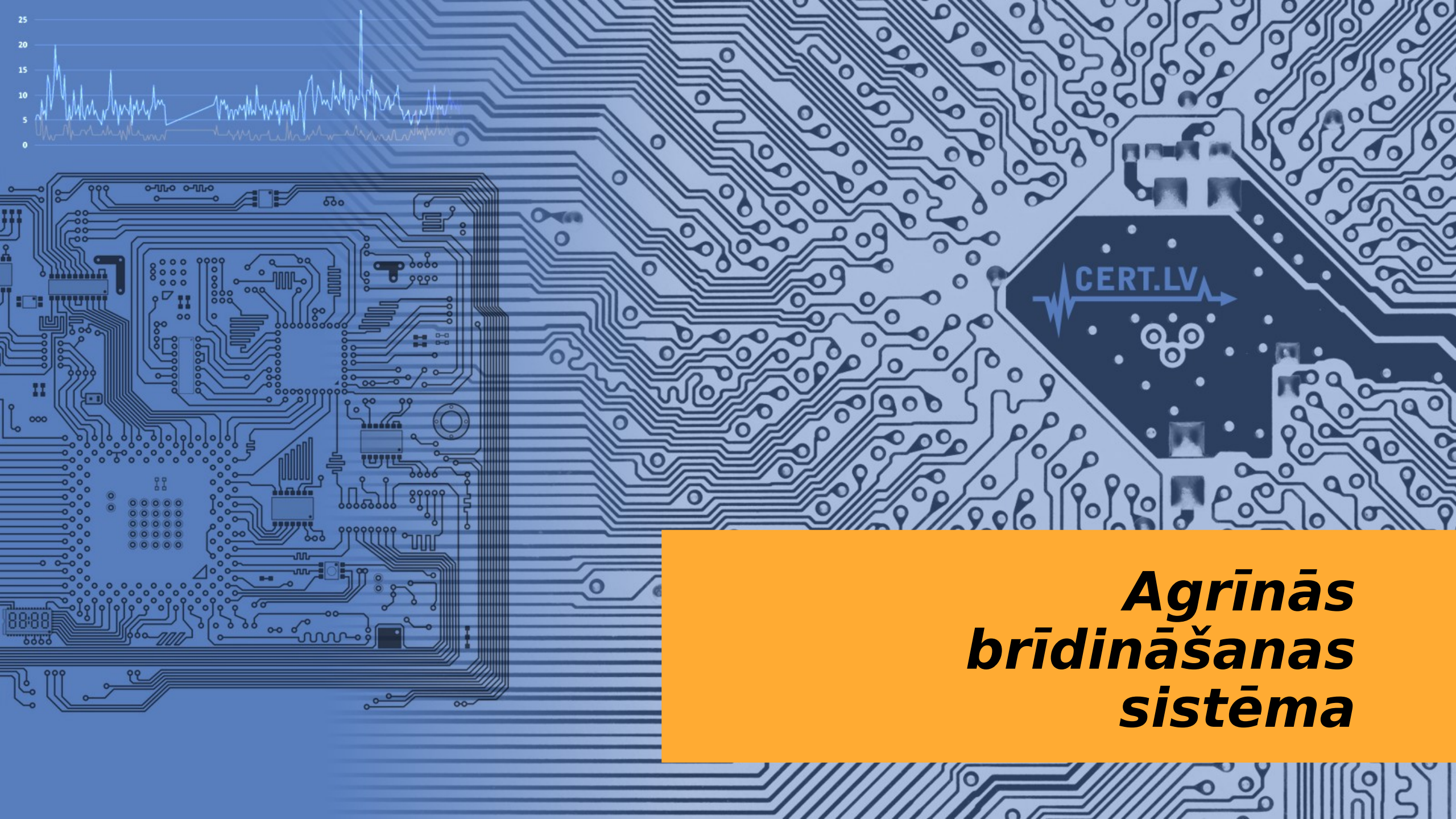
- Izmantot NIC.LV rekursīvo DNS serveri

91.198.156.20

- Uzstādot savu DNS RPZ lokāli un saņemt dinamiskos atjauninājumus no CERT.LV

E-pasts: cert@cert.lv

Subj: **DNS Ugunsmūris**

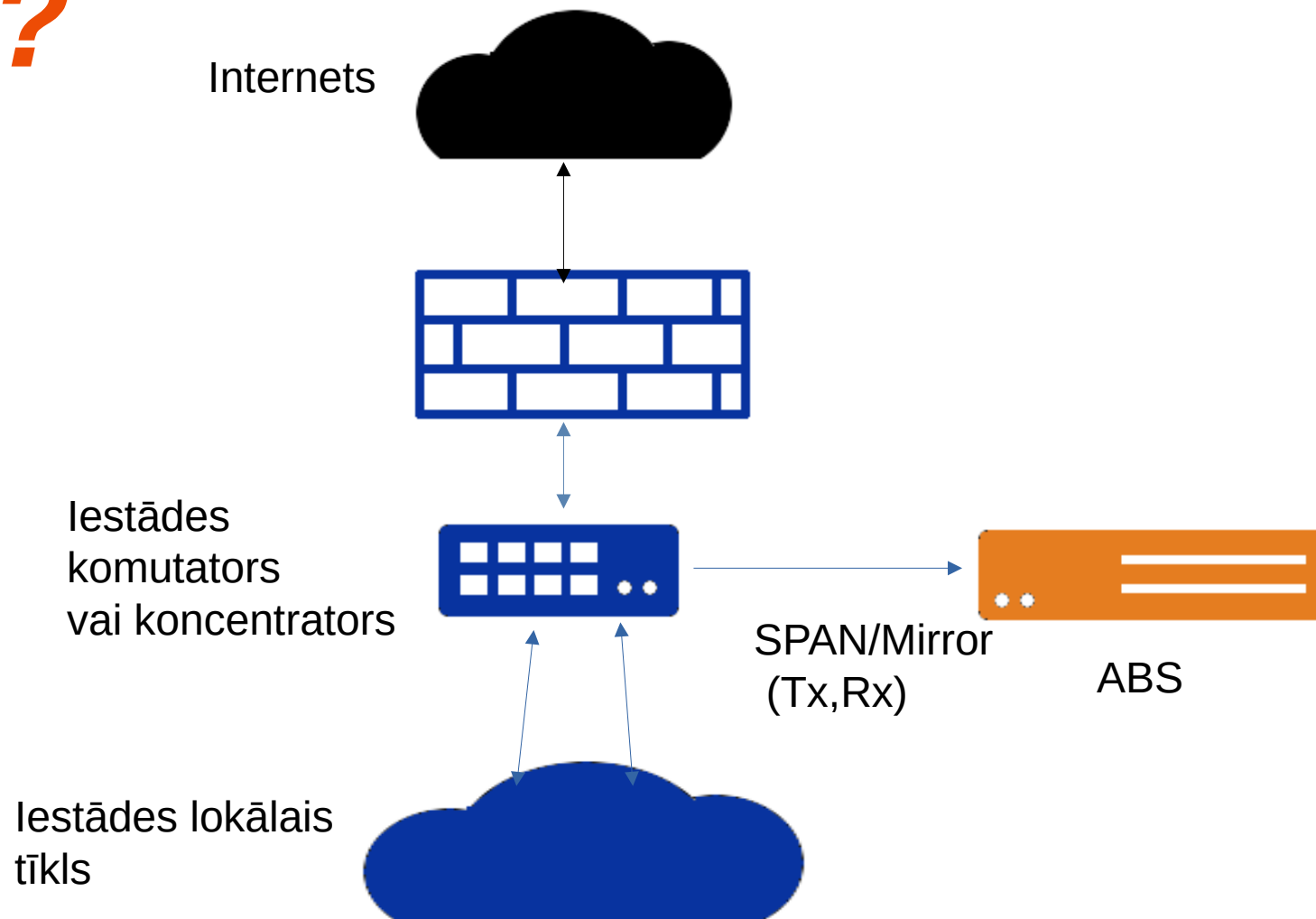


Agrinās brīdināšanas sistēma

Kas tas ir?

- ABS ir serviss, kur tiek analizēta tīkla datu plūsmas kopija, kur pēc predefinētiem noteikumiem tiek atklātas anomālijas.

Ko tas dara?



leguvumi

- Plašāks redzesloks par Jūsu tīklā notiekošo
- Kaitīgā tīkla trafika identificēšana pēc parametriem kā:
 - [IP], [TCP], [UDP]. [DNS], [HTTP], [SSL], [ICMP] u.c.

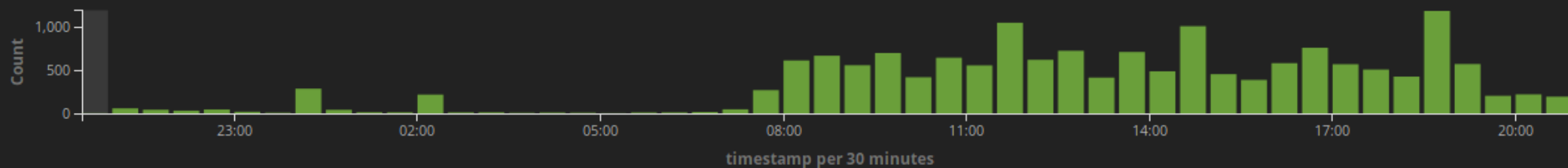
Count



Histogram

16,724

Count



Top signatures



Top categories



Top source IPs

alert.signature.keyword: Descending ▾

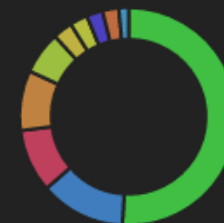
Count ▾

POLICY Android Device (KitKat OS) Connectivity Check	5,259
POLICY Android Device (Marshmallow OS) Connectivity Check	4,254
P2P BitTorrent transfer	1,800
POLICY TeamViewer DynGate Remote Access Checkin	1,212
INFO Session Traversal Utilities for NAT (STUN Binding Response)	946
POLICY HTTP Outbound Request contains pw	888
MALWARE Suspicious User-Agent (1 space)	642
P2P BitTorrent DHT ping request	409
POLICY Dropbox.com Offsite File Backup In Use	311
POLICY TeamViewer Dyngate User-Agent	147

alert.category.keyword: Descending ▾

Count ▾

Potential Corporate Privacy Violation	14,977
Attempted User Privilege Gain	964
A Network Trojan was detected	740
Executable code was detected	25
Web Application Attack	10
Attempted Administrator Privilege Gain	8



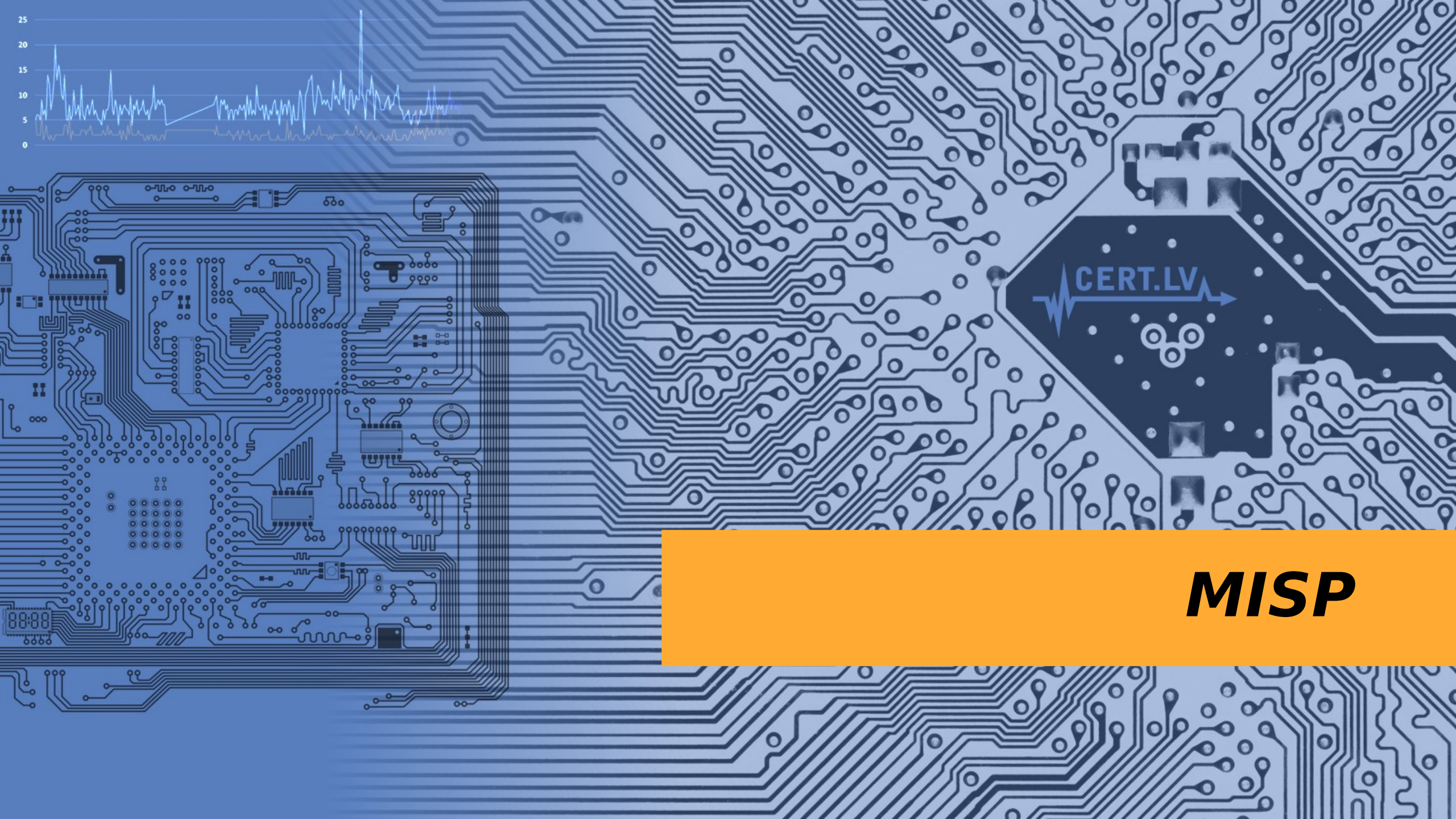
Top destination IPs

Export: [Raw](#) [Formatted](#) Export: [Raw](#) [Formatted](#)

Kā pieteikties?

E-pasts: cert@cert.lv

Subj: **ABS pieteikums**



MISP

Kas tas ir?

Risinājums, kas nodrošina indikatoru glabāšanu, koplietošanu un izmnatošanu no kiberdrošības incidentiem vai ļaunatūras analīzēm.

List Events

Add Event

Import from...

REST client

List Attributes

Search Attributes

View Proposals

Events with proposals

Export

Automation

Events

« previous next »



My Events

Org Events

Filter

☐	Published	Org	Owner Org	Id	Clusters	Tags	#Attr.	#Corr.	Email	Date	Info	Distribution	Actions
☐	✕	TestOrg	TestOrg	3		tlp:amber ecsirt:malicious-code="malware"	6		armins@palms.misp	2019-03-28	Testa notikums	Connected	
☐	✓	TestOrg	TestOrg	2		tlp:white circl:incident-classification="phishing"	3	1	armins@palms.misp	2019-03-28	Viltus lapa	Connected	
☐	✓	TestOrg	TestOrg	1		tlp:green ecsirt:malicious-code="malware"	4	1	armins@palms.misp	2019-03-28	Kkāds notikums	All	

Page 1 of 1, showing 3 records out of 3 total, starting on record 1, ending on 3

« previous next »

[Add Event](#)

✕ 3: Testa ...

Galaxies

Add

« previous

next »

[view all](#)

+



Filters:

All

File

Network

Financial

Proposal

Correlation

Warnings

Deleted

Context

Related Tags



Date ↑

Org

Category

Type

Value

Tags

Galaxies

Comment

Correlate

Related
Events

Feed hits

IDS

Distribution

Sightings



2019-03-28

External analysis

url

http://arejasaiteuzanalizivairesursu.lv
/index.php?id=123

Add



Inherit

(0/0/0)

2019-03-28

Other

comment

Kautkāds komentārs



Add



Inherit

(0/0/0)

2019-03-28

Network activity

domain

cert.lv



Add



Inherit

(0/0/0)

2019-03-28

Network activity

domain

example.com



Add



Inherit

(0/0/0)

2019-03-28

Network activity

domain

testtesttestmalware.com



Add



Inherit

(0/0/0)

2019-03-28

Network activity

ip-dst

10.6.7.8



Add



Inherit

(0/0/0)

« previous

next »

[view all](#)

Quote

Event

Thread

Link

Code

PyMISP

MISP ir REST API funkcionalitāte

PyMISP – Python bibliotēkas darbam ar MISP:

[lasīt], [rakstīt], [filtrēt], [pārbaudīt] u.c.

```
    "name": "MyOrg",
    "uuid": "5c62bfd0-0a2c-4a42-ae99-466da5c095de"
  },
  "Orgc": {
    "id": "1",
    "name": "MyOrg",
    "uuid": "5c62bfd0-0a2c-4a42-ae99-466da5c095de"
  },
  "Attribute": [
    {
      "id": "1",
      "type": "domain",
      "category": "Network activity",
      "to_ids": true,
      "uuid": "5c9bbddf-7e08-436c-949f-04d5c0a83865",
      "event_id": "1",
      "distribution": "5",
      "timestamp": "1553710047",
      "comment": "Komentaars",
      "sharing_group_id": "0",
      "deleted": false,
      "disable_correlation": false,
      "object_id": "0",
      "object_relation": null,
      "value": "example.com",
      "Galaxy": [],
      "ShadowAttribute": []
    },
    {
      "id": "2",
      "type": "domain",
      "category": "Network activity",
      "to_ids": true,
      "uuid": "5c9bbc06-54d0-4baf-9111-0556a5c095de",
      "event_id": "1"
```

leguvumi.

- Būt lietas kursā par apdraudējumiem
- Vienkāršāk padalīties ar adraudējumiem
- Automizācija un integrācija ar savām sistēmām

Kā pieteikties?

MISP “nāk līdzi” ar ABS

E-pasts: cert@cert.lv

Subj: **ABS, MISP pieteikums**

DNS Ugunsmūris

DNS: 91.198.156.20



Paldies!

cert@cert.lv

<https://www.cert.lv>



certlv



certlv



**Līdzfinansē Eiropas Savienības Eiropas
infrastruktūras savienošanas instruments**