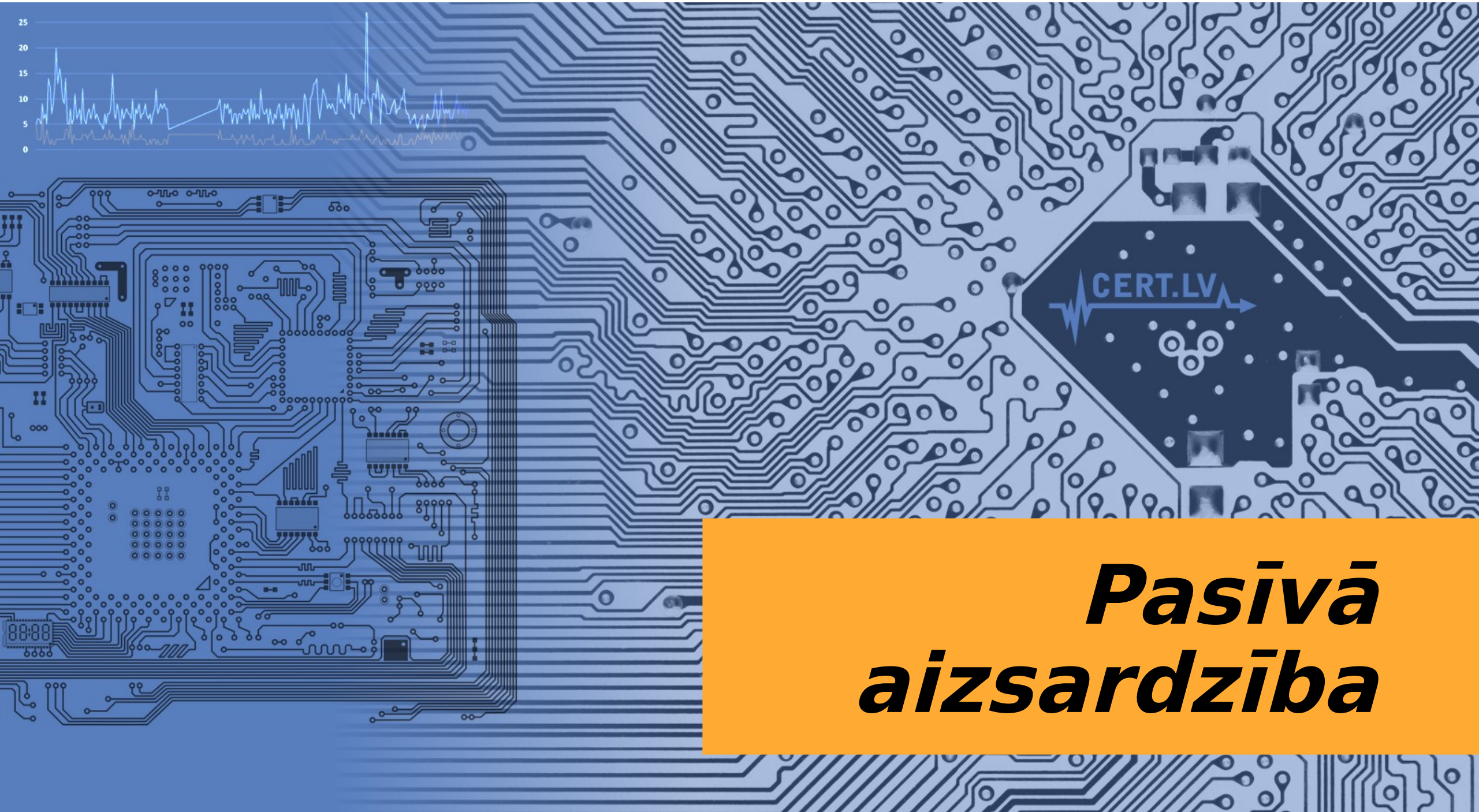
CERT.LV

Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

CERT.LV piedāvātie drošības risinājumi

Armīns Palms, CERT.LV



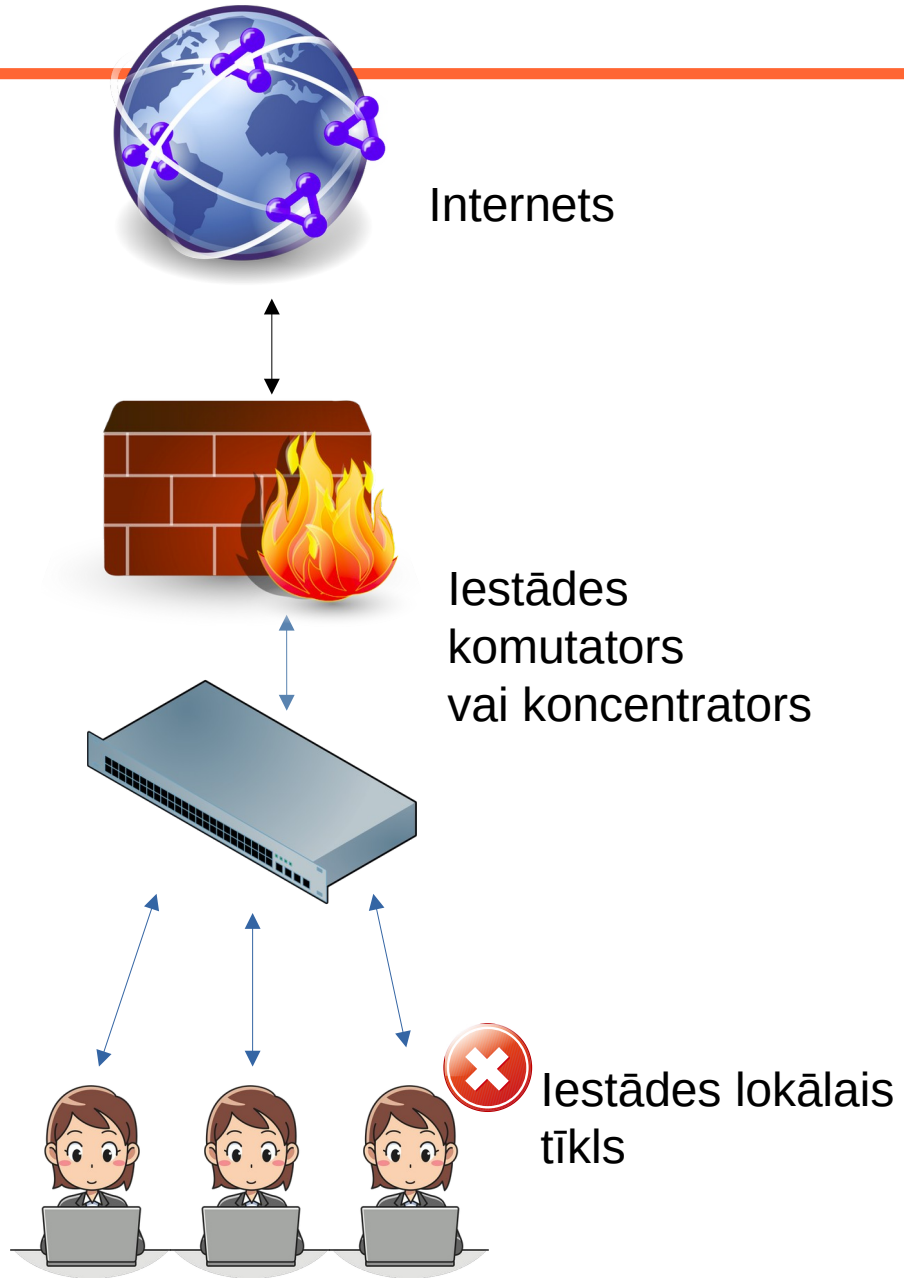
Pasīvā aizsardzība

Ja vēlies...

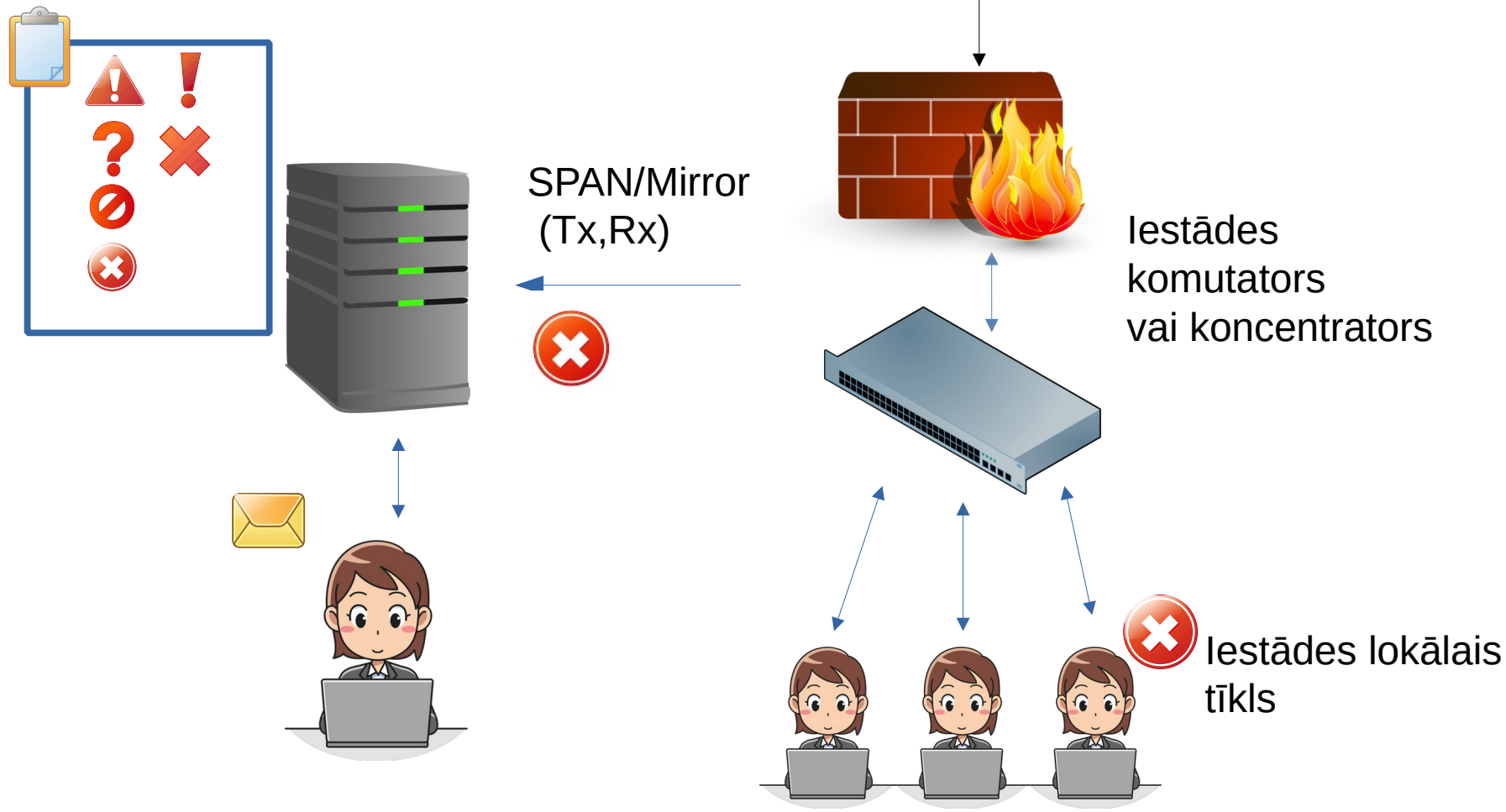
- **zināt, kas notiek Tavā tīklā**
- **tikt informēts, ja ir noticis incidents**
- **personalizētu tīkla monitoringu**
- **pārskatāmu saskarni par notikumiem**
- **atklāt anomālijas, kurām nav signatūru**

Agrās brīdināšanas sistēma

Ko tas dara?


Internets
Iestādes
komutators
vai koncentrators
Iestādes lokālais
tīkls

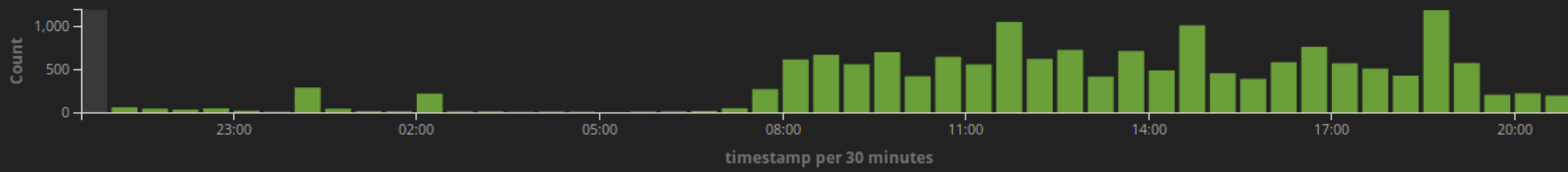
Ko tas dara?


Internets
SPAN/Mirror
(Tx,Rx)
Iestādes
komutators
vai koncentrators
Iestādes lokālais
tīkls

Count

16,724
Count

Histogram



Top signatures

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

Export: Raw Formatted

Top categories

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

Export: Raw Formatted

Top source IPs

Top destination IPs

Ieguvumi

- **Informācija par Jūsu tīklā notiekošo**
- **Kaitīgo datu plūsmas identificēšana pēc pavedieniem kā: [IP], [TCP], [UDP]. [DNS], [HTTP], [SSL], [ICMP] u.c.**
- **Apdraudējumu indikatoru atjauninājumi**
- **CERT.LV atbalsts**
- **MISP**

MISP


MISP
Threat Sharing
IP
EVENT A
EVENT B
UI USERS
Database
API USERS
API
MISP XML and JSON
OpenIOC
STIX XML and JSON (export)
Suricata export
Snort export
CSV export
GFI import

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
2019-03-28		External analysis	url	http://arejasaiteuzanalizivairesursu.lv/index.php?id=123	+	Add		✓			
2019-03-28		Other	comment	Kautkāds komentārs	+	Add		✓			
2019-03-28		Network activity	domain	cert.lv	+	Add		✓			✓
2019-03-28		Network activity	domain	example.com	+	Add		✓			✓
2019-03-28		Network activity	domain	testtesttestmalware.com	+	Add		✓			✓
2019-03-28		Network activity	ip-dst	10.6.7.8	+	Add		✓			✓

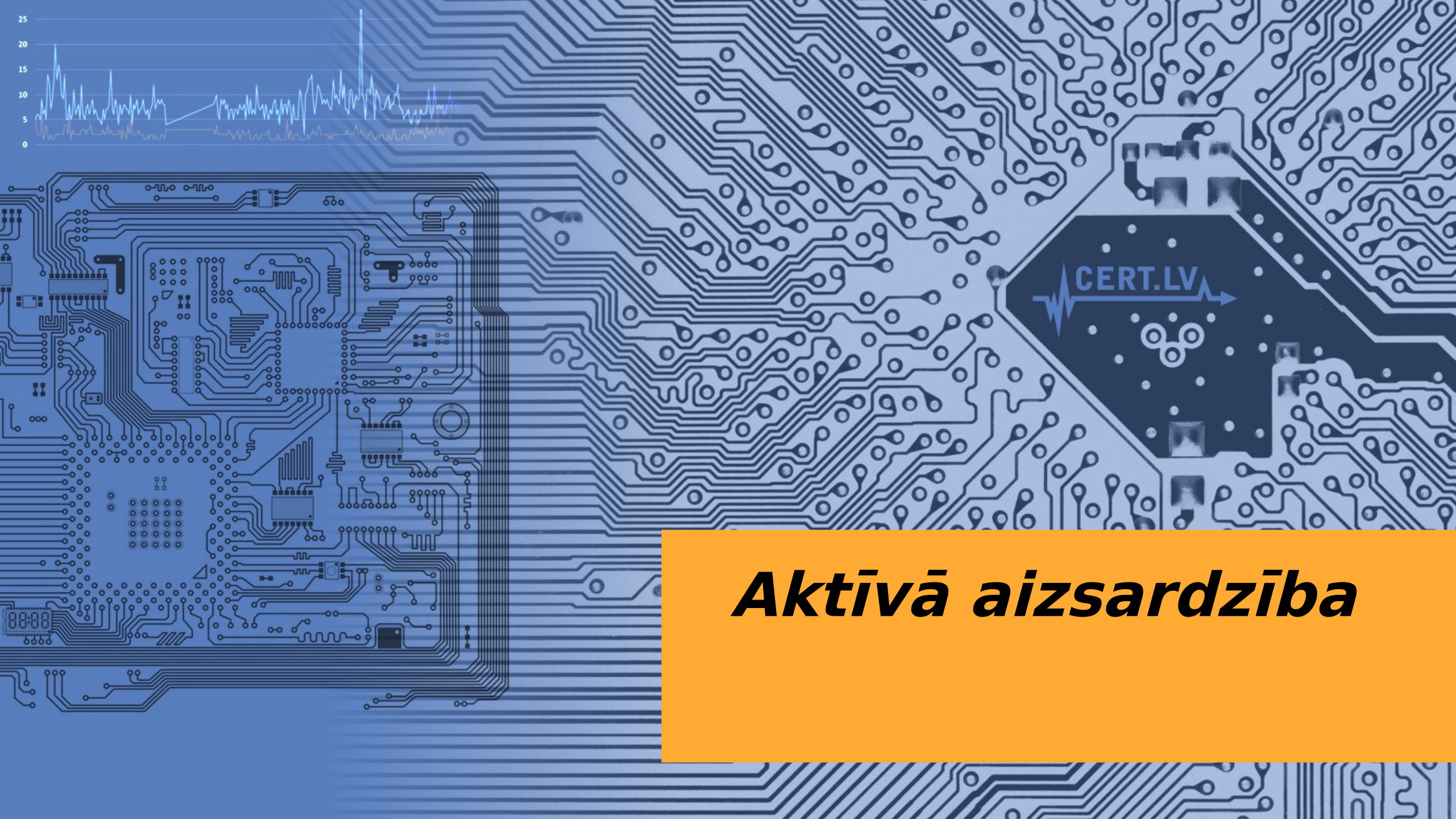
```
    "name": "MyOrg",
    "uuid": "5c62bfd0-0a2c-4a42-ae99-466da5c095de"
  },
  "Orgc": {
    "id": "1",
    "name": "MyOrg",
    "uuid": "5c62bfd0-0a2c-4a42-ae99-466da5c095de"
  },
  "Attribute": [
    {
      "id": "1",
      "type": "domain",
      "category": "Network activity",
      "to_ids": true,
      "uuid": "5c9bbbdf-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",
```

Kā pieteikties?

MISP “nāk līdzi” ar ABS

E-pasts: **cert@cert.lv**

Subj: **ABS, MISP pieteikums**



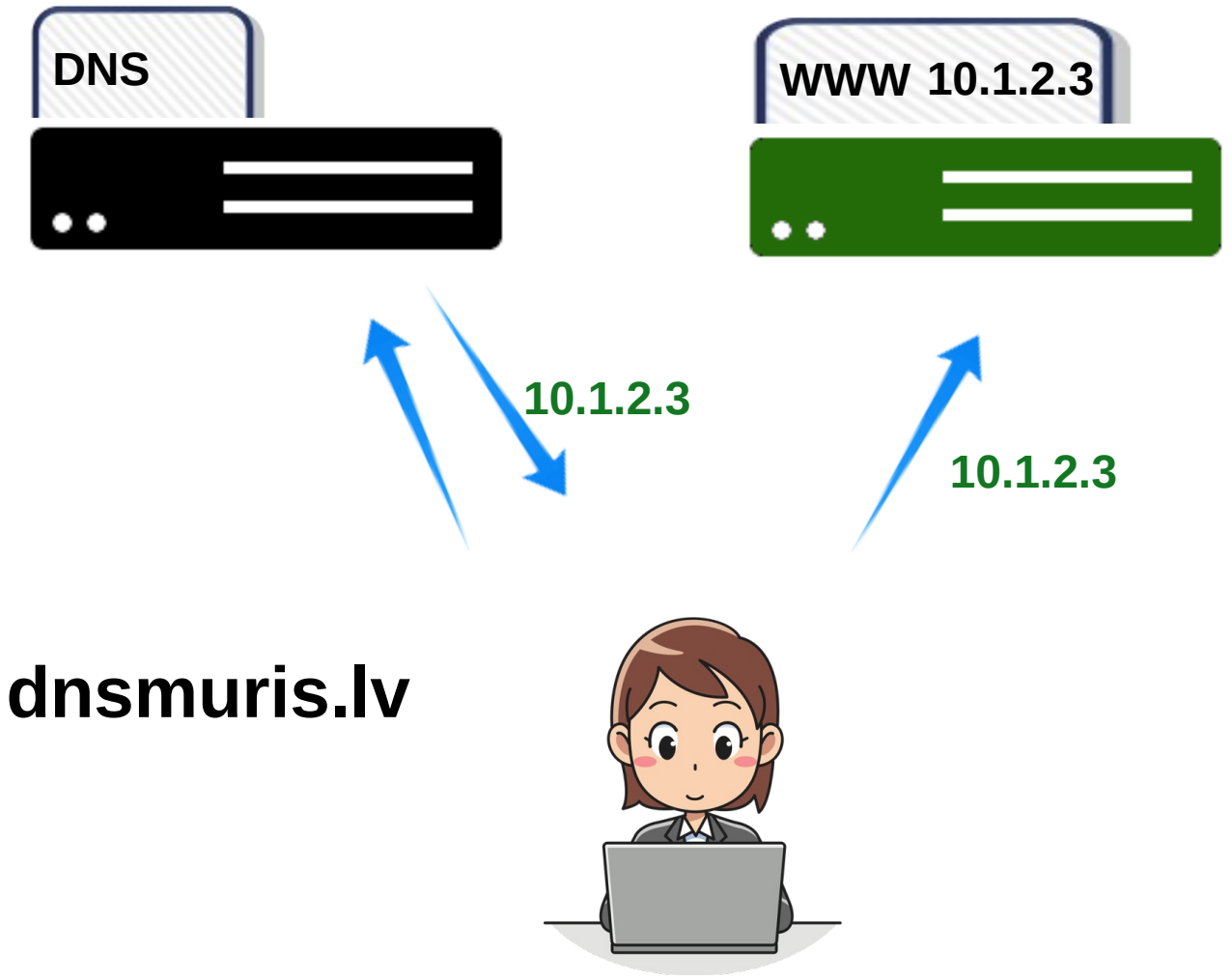
Aktīvā aizsardzība

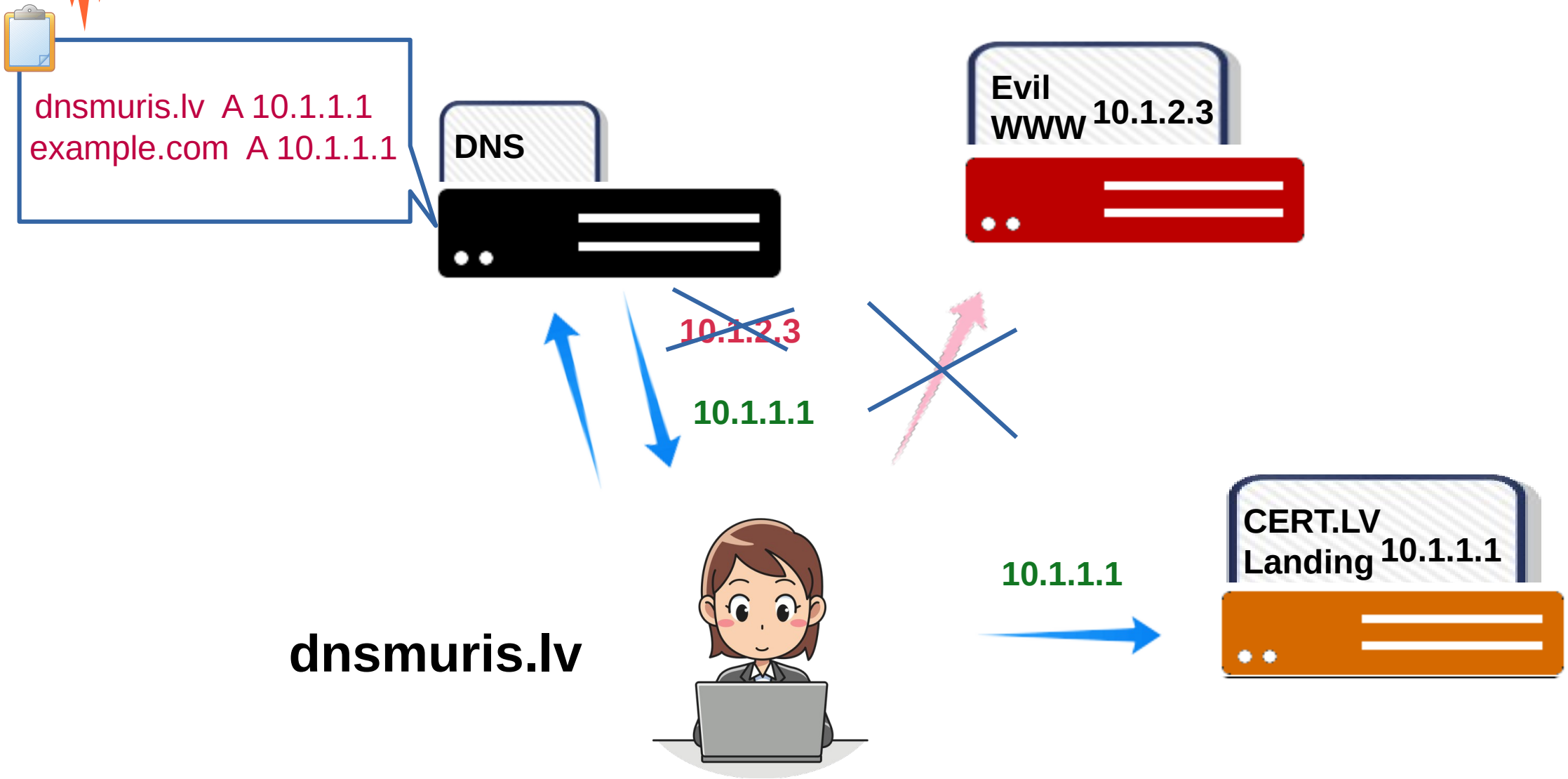
Ja vēlies...

- **vienkārši lietojamu aizsardzības risinājumu**
- **aizsardzību mājās, darbā, uzņēmumā**
- **aizsardzību no aktuālām kampaņām Latvijā un pasaulē**

DNS Ugunsmūris

dnsmuris.lv

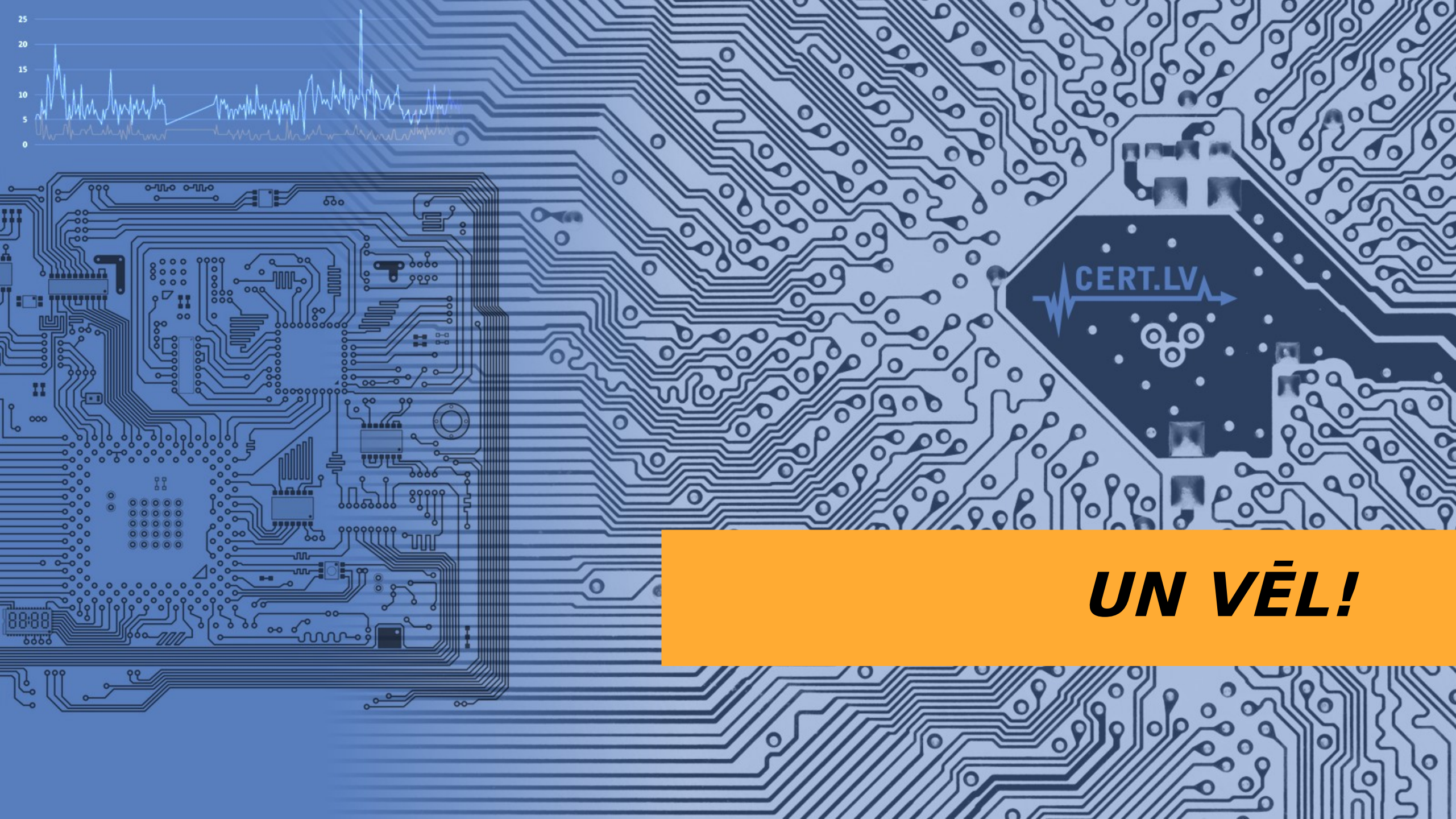

DNS
WWW 10.1.2.3
10.1.2.3
10.1.2.3
dnsmuris.lv


dnsmuris.lv A 10.1.1.1
example.com A 10.1.1.1
DNS
Evil
WWW 10.1.2.3
10.1.2.3
10.1.1.1
dnsmuris.lv
10.1.1.1
CERT.LV
Landing 10.1.1.1

DNS Ugunsmūris

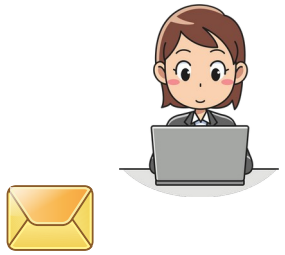
DNS: 91.198.156.20

dnsmuris.lv

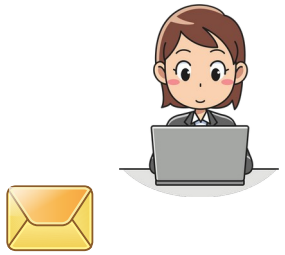

25
20
15
10
5
0
CERT.LV
UN VĒL!

Ja vēlies...

- **Būt informēts par savas iestādes IT infekcijām un apdraudējumiem**

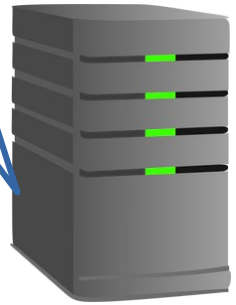


Iestāde A



Iestāde B

10.1.1.5 spamo
10.2.2.10 bots
10.3.3.4 openresolver
10.4.4.8 openrdp



Iestāde A: 10.1.1.0/24

Iestāde B: 10.2.2.0/24

Paldies!

cert@cert.lv

https://www.cert.lv

certlv **certlv**

Līdzfinansē Eiropas Savienības Eiropas infrastruktūras savienošanas instruments