CERT.LV pakalpojumu grozs

12.12.2023.

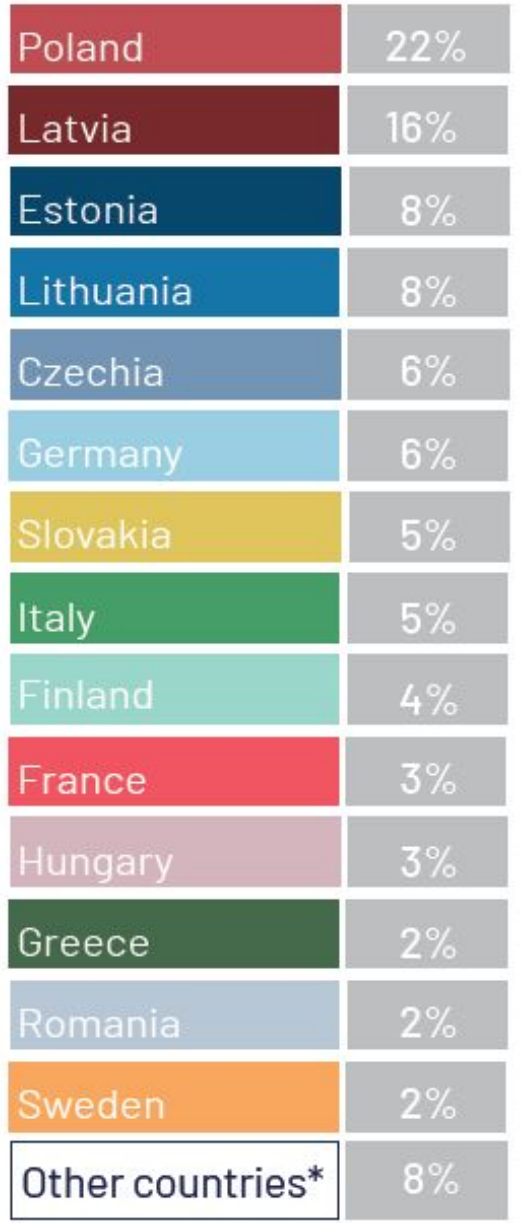
Varis Teivāns

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Krievijas uzbrukumu intesitāte ES valstīm

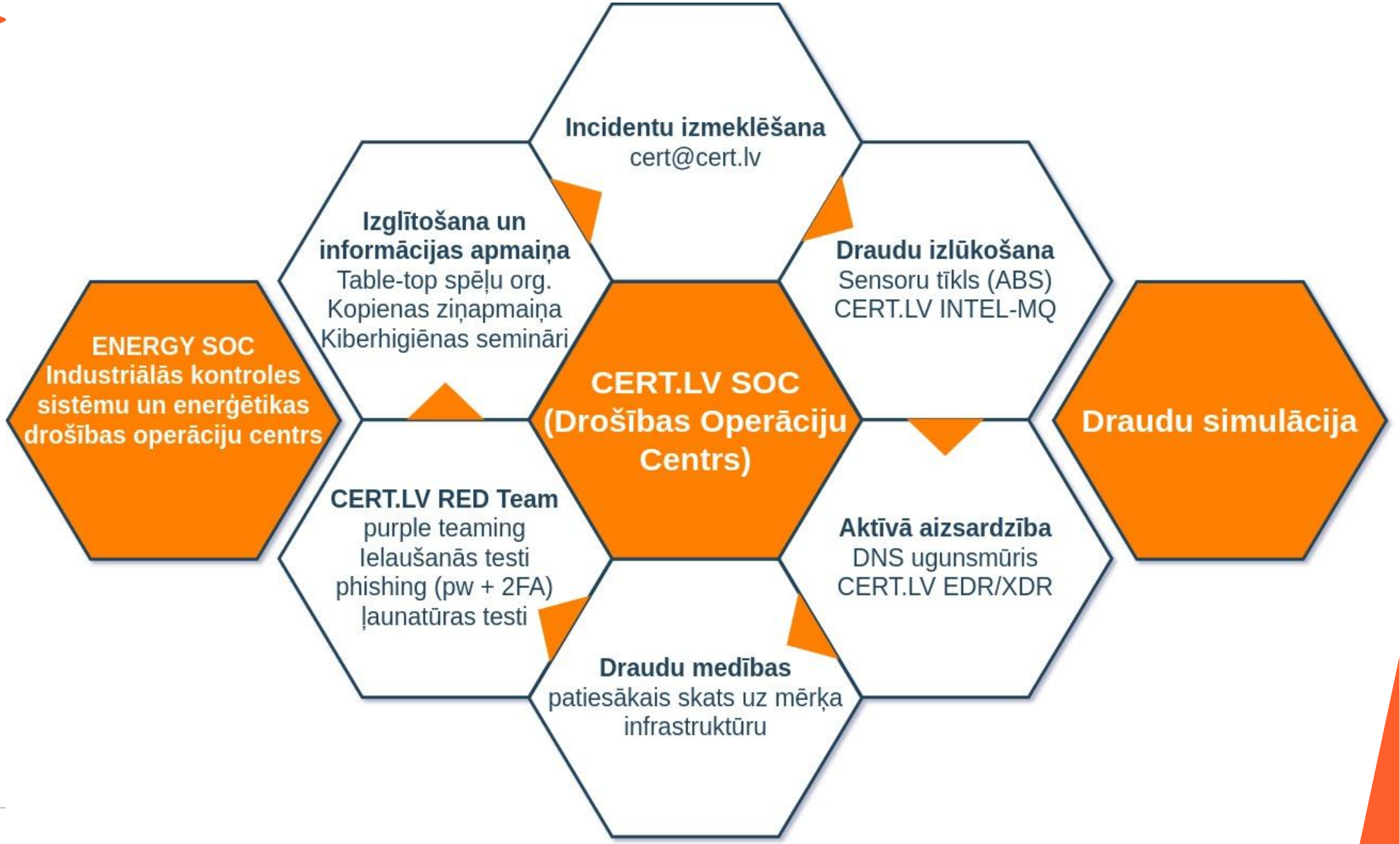
CERT-EU aggregated data (most attacked countries)

RUSSIA'S WAR ON UKRAINE: ONE YEAR OF CYBER OPERATIONS

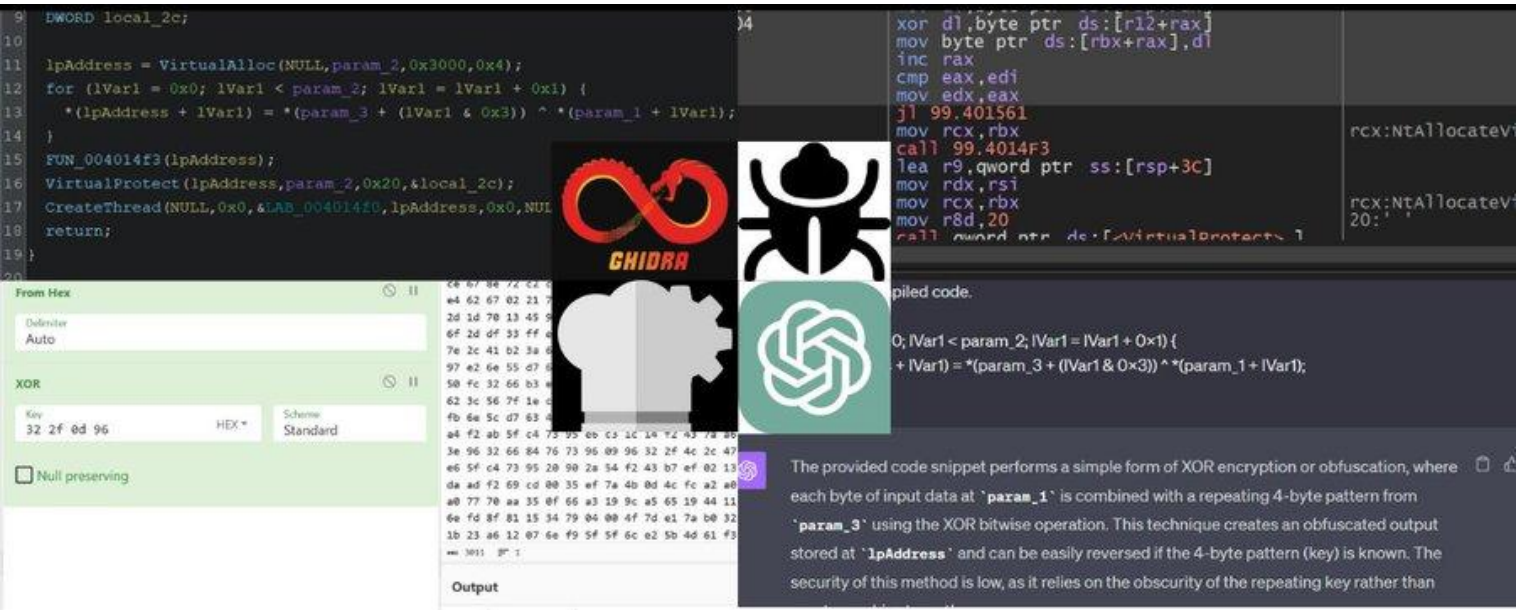



ENERGY SOC
Industriālās kontroles sistēmu un enerģētikas drošības operāciju centrs
CERT.LV SOC
(Drošības Operāciju Centrs)
Draudu simulācija

CERT.LV


Incidentu izmeklēšana
cert@cert.lv
Izglītošana un informācijas apmaiņa
Table-top spēļu org.
Kopienas ziņapmaiņa
Kiberhigiēnas semināri
Draudu izlūkošana
Sensoru tīkls (ABS)
CERT.LV INTEL-MQ
ENERGY SOC
Industriālās kontroles sistēmu un enerģētikas drošības operāciju centrs
CERT.LV SOC (Drošības Operāciju Centrs)
Draudu simulācija
CERT.LV RED Team
purple teaming
Ielaušanās testi
phishing (pw + 2FA)
ļaunatūras testi
Aktīvā aizsardzība
DNS ugunsmūris
CERT.LV EDR/XDR
Draudu medības
patiesākais skats uz mērķa infrastruktūru

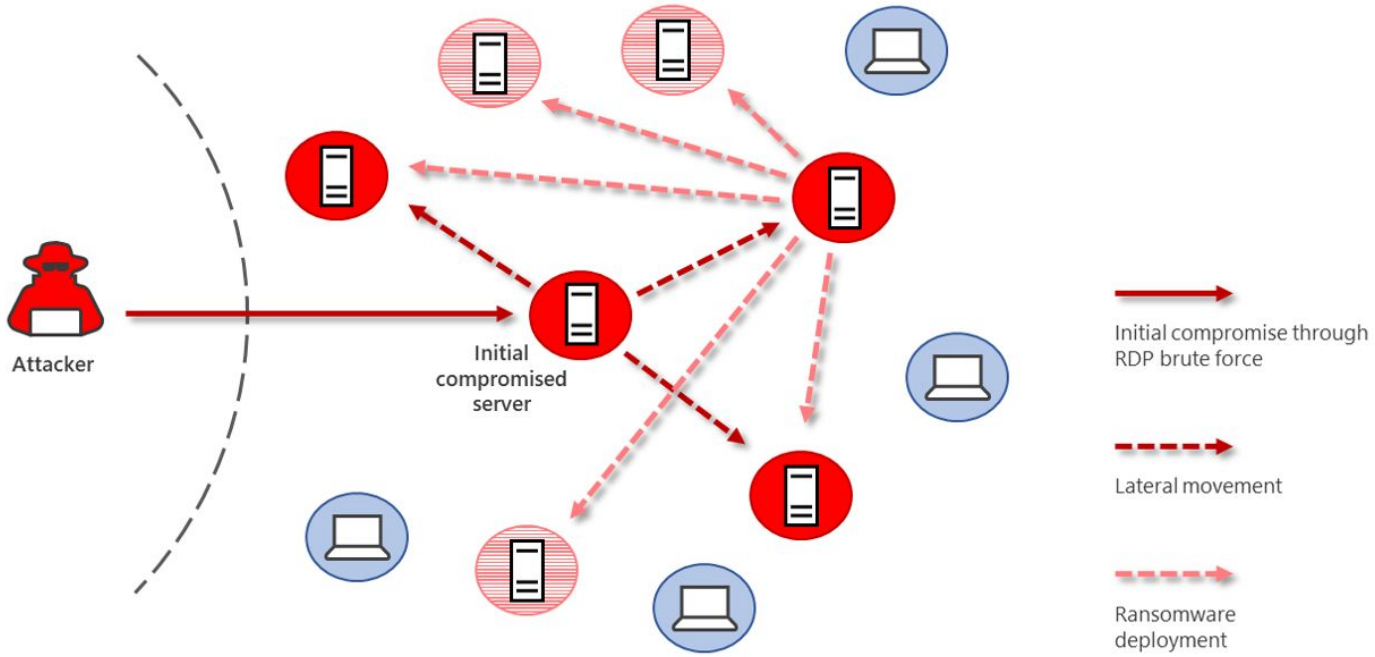
- **Vairāk kā 6,5 miljoni telemetrijas signālu mēnesī**
  - Automatizācija
- **15-20 manuāli risināti incidenti katru dienu**
- **Incidentu izmeklēšanas atbalsts pieejams ikvienam**
  - Prioritātes: NIS2 direktīvas subjekti, cita kritiskā infrastruktūra un būtisko pakalpojumu sniedzēji, publiskais sektors
  - Ikviens Latvijas iedzīvotājs - saziņa cert@cert.lv; +371 67085888



- **Draudu izlūkošanas procesi integrēti Incidentu Reaģēšanas komandā**
  - Kolektīvās aizsardzības principi
  - Jautājumi, kurus uzdodam, monitorejot uzbrucēju saziņas kanālus un rīkus:
    - Kam uzbrūk, kādā veidā, vai varam apsteigt un pretdarboties
    - Vai varam dalīties ar konstatēto
    - Kas uzbrūk un ko dara, ja izdodas
    - Vai varam mazināt kaitējumu
    - Uzbrucēja maldināšanas taktikas
  - CERT.LV ir valstī lielākais draudu telemetrijas akumulators
    - Cenšamies gūt maksimālu labumu valsts drošībai no apstrādātās informācijas
    - Vienota un sektorāla apdraudējuma līmeņa noteikšana

- **DNS ugunsmūris pakalpojuma mērķi**
  - Nodrošināt valstī vienotu bloķējamo domēnu zonu apstrādi un izplatīšanu
  - Nodrošināt aktīvu aizsardzību ikvienam
- **Kā un kas var lietot?**
  - Ikviens iedzīvotājs bez jebkādām saistībām - NIC.LV rekursīvie serveri: IPv4: 91.198.156.20, IPv4: 194.8.2.2. informāciju meklē https://dnsmuris.lv
  - Slēdzot līgumu, CERT.LV DNS RPZ zonas sinhronizācija ar iestādes infrastruktūru
  - Android un iOS lietotnes 2024. gadā
- **Statistika**
  - Gandrīz 1 miljons aizsargātu/nobloķētu DNS pieprasījumu gadā
  - 1,5 miljons apstrādātu DNS pieprasījumu mēnesī
- **Augstas kvalitātes pakalpojums**
  - Gada laikā tikai 5 false positive domēnu bloķēšanas gadījumi

- **CERT.LV EDR/XDR pakalpojuma mērķi**
  - Savlaicīgi identficēt, mazināt un apturēt kiberapdraudējuma kaitējumu
- **Divi attīstības virzieni**
  - Valsts nozīmes datu centru drošības telemetrija
  - Publiskā sektora korporatīvo tīklu, gala iekārtu drošība



- **Latvija ir līderis draudu medību operāciju vadīšanā ES**
  - Teicama sadarbība ar
    - Kanādas NBS un Kiberdrošības centru
    - ASV kiberpavēlniecību
- **Vairāk kā 100 000 analizētu gala iekārtu**
  - Identificēti un no mērķa infrastrukturas neitralizēti Krievijas, Ķīnas un komerciāli motivēti draudu aktieri

- **Mērķauditorija**
  - Valsts iestādes
  - Kritiskā infrastruktūra un būtisko pakalpojumu sniedzēji
  - Mērķa iestādes izvēle sadarbībā ar valsts drošības iestādēm
  - Iespēja pieteikt draudu medības cert@cert.lv

RED Team kā izdalīts CERT.LV darbības virziens

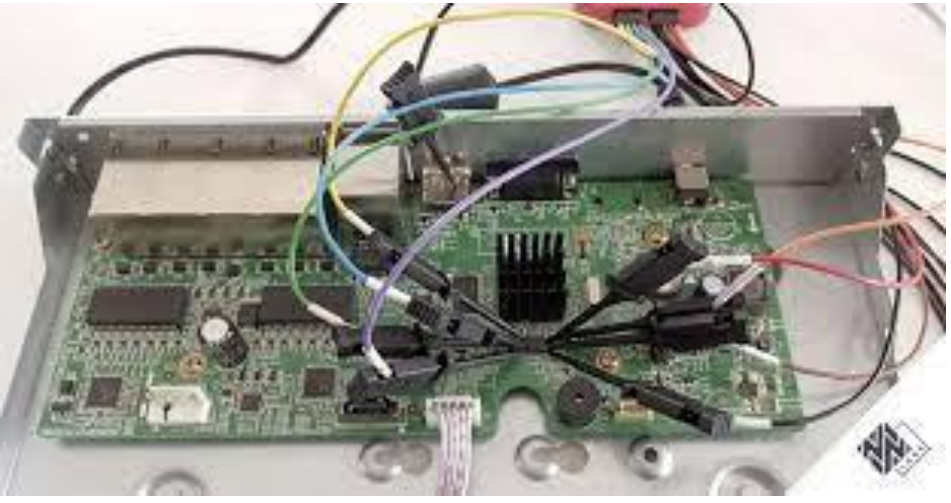
- Ielaušanās testi (WEB, API, Tīkla perimetrs, Android, u.c.)
- Pikšķerēšanas testi un atgriezeniskā saite
- Ļaunatūras (nekaitīgas) piegādes testi un atgriezeniskā saite

Mērķauditorija:

- NIS2 direktīvas subjekti, KI
- Būtisko pakalpojumu sniedzēji
- Publiskais sektors

- **Vairāk kā 10 000 apmācīto personu katru gadu**
- **Kiberdrošības galda mācības (table-top)**
- **Latvijas kiberdrošības kopienas ziņapmaiņa https://mm.cert.lv**
    - **Pieteikties cert@cert.lv ar rekomendāciju no esoša biedra**

- **Industriālo kontroles sistēmu mezglu un sakaru protokolu drošības testi**
- **Transporta, Ūdens, Gāzes, Elektrības, citu nozaru industriālās automatizācijas infrastruktūras testēšana**
- **Industriālo kontroles sistēmu drošības laboratorija**
- **IDS sensora prototips ar ML integrāciju**



ENERGY SOC
Industriālās kontroles sistēmu un enerģētikas drošības operāciju centrs

- **Draudu aktieru rīku, metožu un procedūru simulācija, identificēšanas spēju testēšana un pilnveidošana**
- **SOC/SIEM/EDR/XDR/MDR spēju, tvēruma, kvalitātes un reakcijas testi**

Mērķauditorija:

- **NIS2 direktīvas subjekti, KI**
- **Būtisko pakalpojumu sniedzēji**
- **Publiskais sektors**

saziņa cert@cert.lv

Paldies par uzmanību!

cert@cert.lv

certlv

certlv