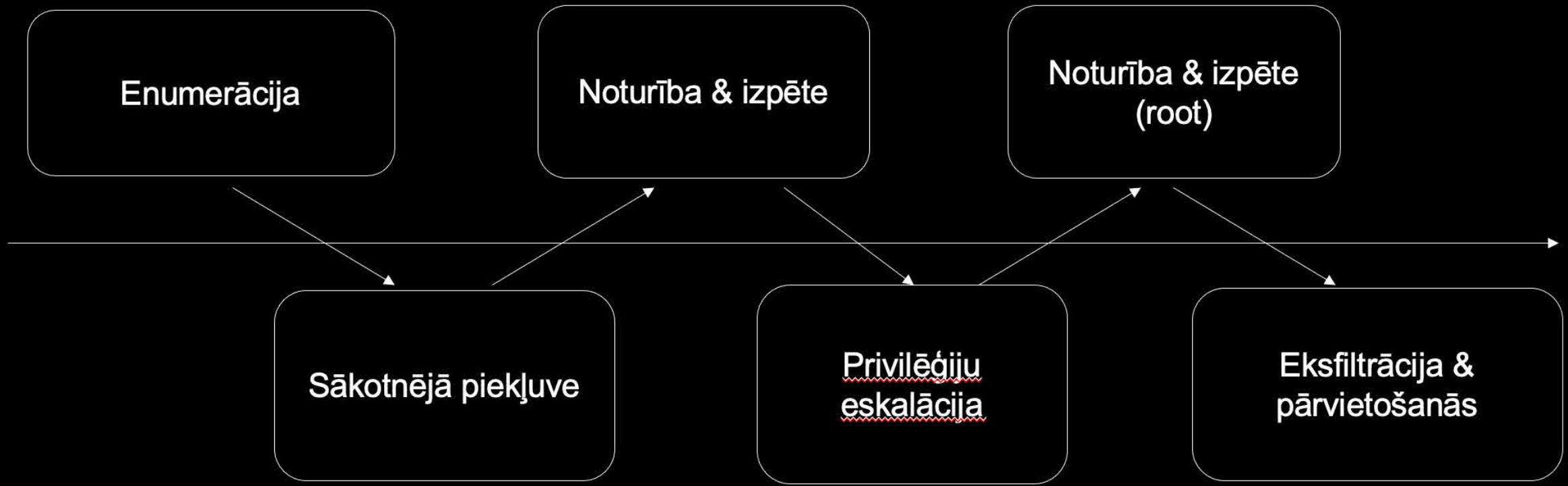
Rīcība incidenta gadījumā

Armīns Palms
17.03.2026.

CERT.LV
Kiberincidentu novēršanas institūcija

Uzbrucēja aktivitātes



Ikdienas rutīna

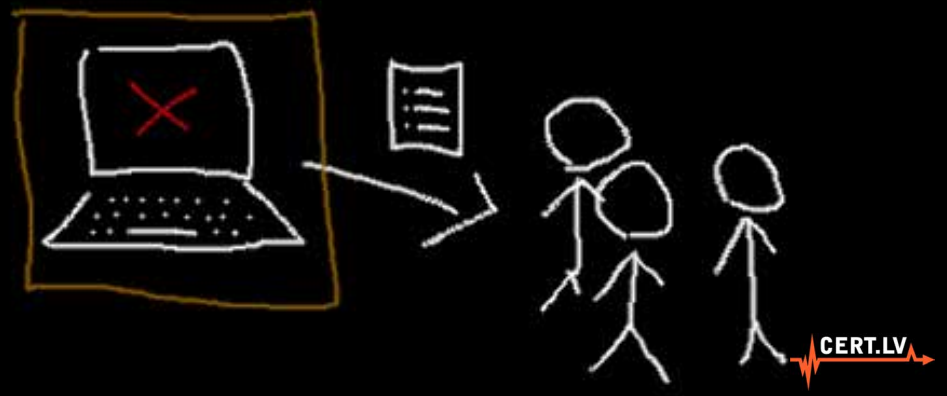
- Veicam darbības, lai uzbrucējiem padarītu grūtu vai neērtu sistēmu
- Gatavojamies kiberincidentam

Incidents

Incidents

- Tūlītējās darbības
  - Situācijas novērtēšana
  - Tehniskās darbības – incidenta sākotnējā novēršana vai minimizēšana
  - Informatīvās darbības – informācija vadībai, sabiedriskās attiecības, kompetentās iestādes u.c.

Incidents – Reakcija



Ziņošanas kārtība

Nacionālā kiberdrošības likuma **subjekti**:			**Citi**
	Ziņošana par **ikdienas** kiberdrošības incidentiem*	Ziņošana par **nozīmīgiem** kiberdrošības incidentiem**	Ziņošana par kiberdrošības incidentiem*
Būtisko pakalpojumu sniedzēji **Svarīgo** pakalpojumu sniedzēji IKT **kritiskās infrastruktūras** īpašnieks vai tiesiskais valdītājs	Par kiberdrošības incidentu, kurš **nav uzskatāms par nozīmīgu**, ziņo kompetentajai kiberincidentu novēršanas institūcijai, nosūtot uz e-pasta adresi cert@cert.lv kiberdrošības incidenta aprakstu brīvā formā	Par kiberincidentu **nekavējoties informē kompetento kiberincidentu novēršanas institūciju** un izpilda tās sniegtos norādījumus par rīcību kiberincidenta gadījumā. **Agrīnais brīdinājums** – 24 stundu laikā **Sākotnējais ziņojums** – 72 stundu laikā **Uzticamības pakalpojumu sniedzējiem** — 24 stundu laikā **Gala ziņojums** – 6 mēnešu laikā pēc sākotnējā ziņojuma iesniegšanas **Progresa ziņojums** – ja 6 mēnešu laikā nav izdevies atrisināt incidentu (pēc incidenta atrisināšanas iesniedz gala ziņojumu)	**Par konstatēto kiberdrošības incidentu** ir iespēja brīvprātīgi ziņot kompetentajai kiberincidentu novēršanas institūcijai, nosūtot aprakstu brīvā formā uz e-pasta adresi cert@cert.lv Kiberincidentu novēršanas institūcija vienojas ar personu, kura ziņojusi par kiberdrošības incidentu, par atbalsta sniegšanu kiberincidenta risināšanā. Kā arī pēc savas iniciatīvas var brīvprātīgi ziņot kompetentajai kiberincidentu novēršanas institūcijai **par gandrīz notikušu kiberincidentu*** ** vai **kiberapdraudējumu*****. Brīvprātīga ziņošana par kiberdrošības incidentu, gandrīz notikušu kiberincidentu vai kiberapdraudējumu neuzliek personai papildu pienākumus.
IKT **kritiskās infrastruktūras** īpašnieks vai tiesiskais valdītājs		Vienlaicīgi informē arī **kompetento valsts drošības iestādi**.	

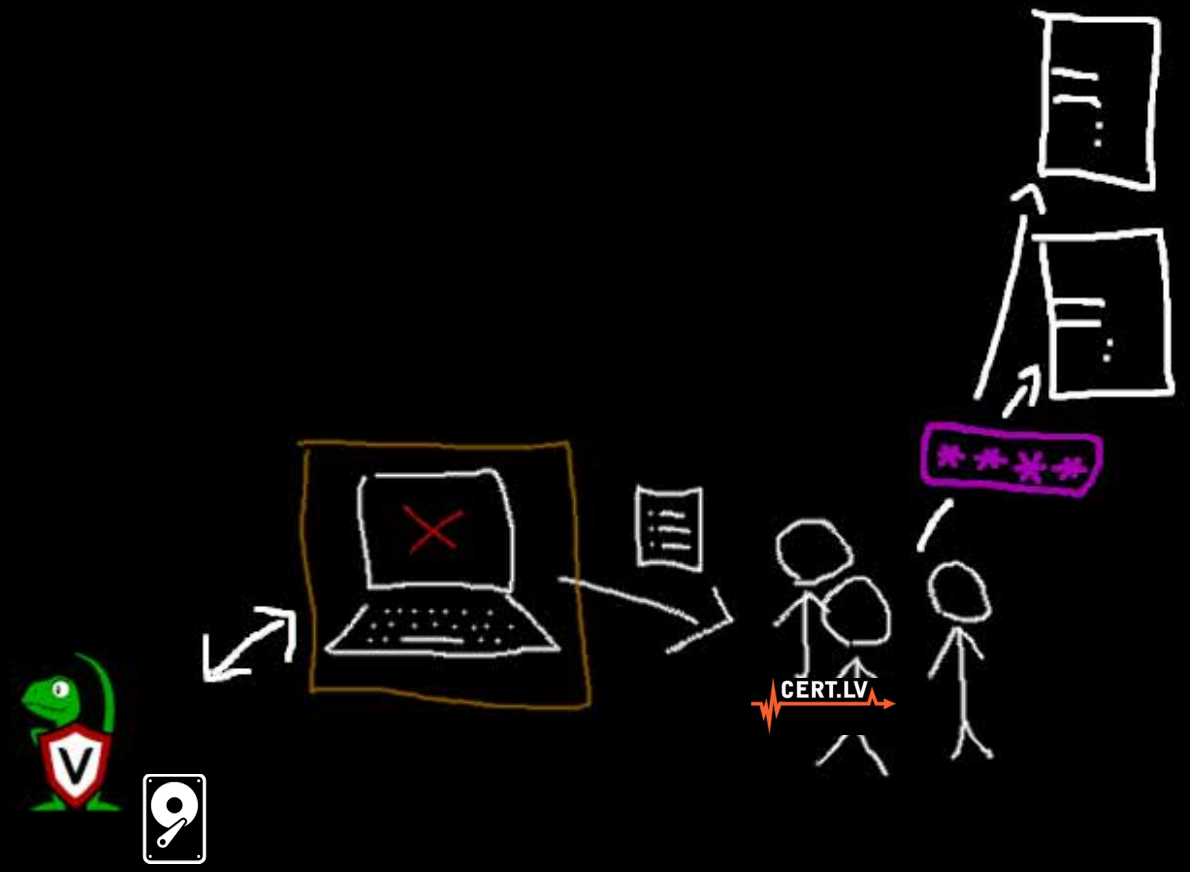
https://cert.lv/lv/riciba-kiberincidenta-gadijuma

Identifikācija

- Ierobežošana!
- Ātrā pierādījumu apkopošana (triage):
  - EVTX
  - Prefetch (programmu izpilde)
  - AmCache (instalētās aplikācijas, to izpilde, draiveru ielāde u.c.)
  - Pārlūka dati (vēsture, sīkdatnes, sesijas)
  - Powershell transcript (jāpārliecinās vai ir)
  - Registry
  - U.C.

- Operatīvās atmiņas kopija
- Spoguļkopija

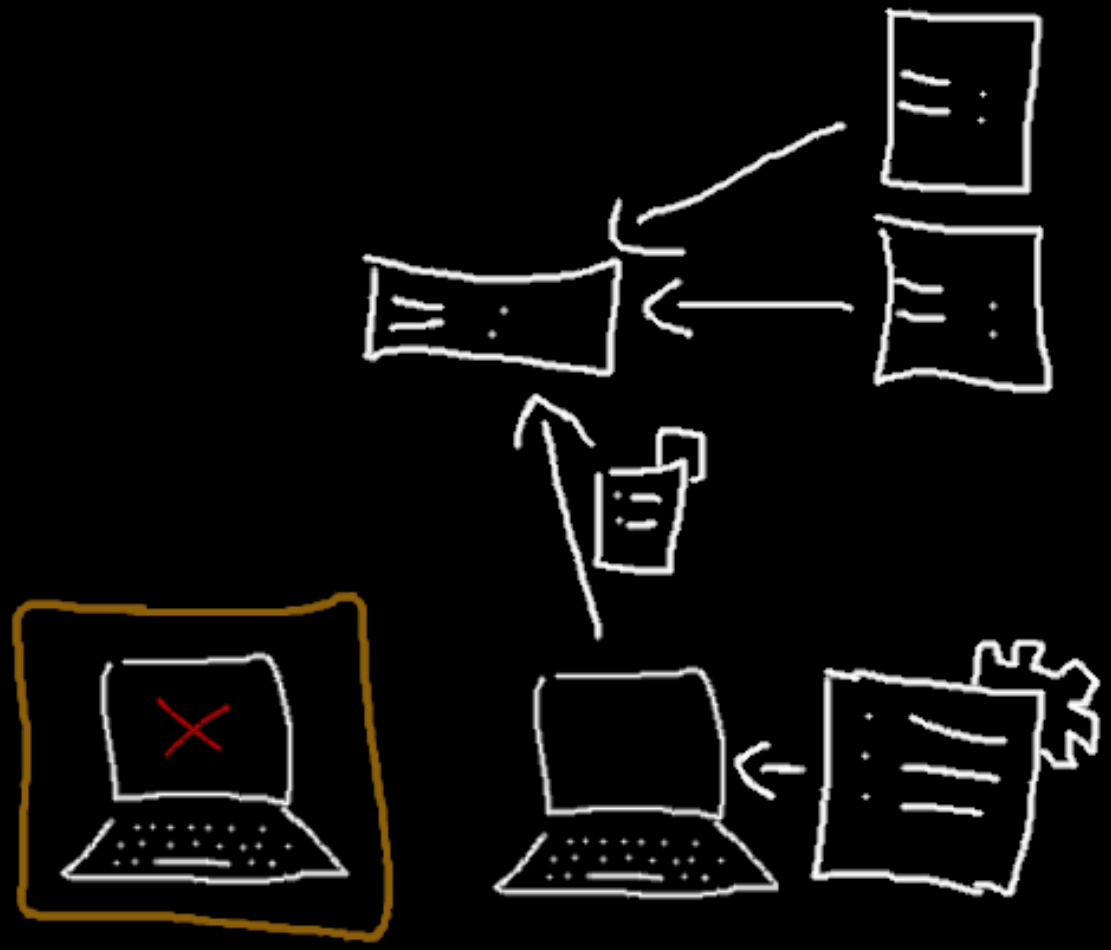
Incidents – Identifikācija -> ierobežošana



Grūtības

- Nepilnīga žurnalēšana
- Iekšējo procedūru trūkums
- Sabojāti pierādījumi
- Dzēsti pierādījumi

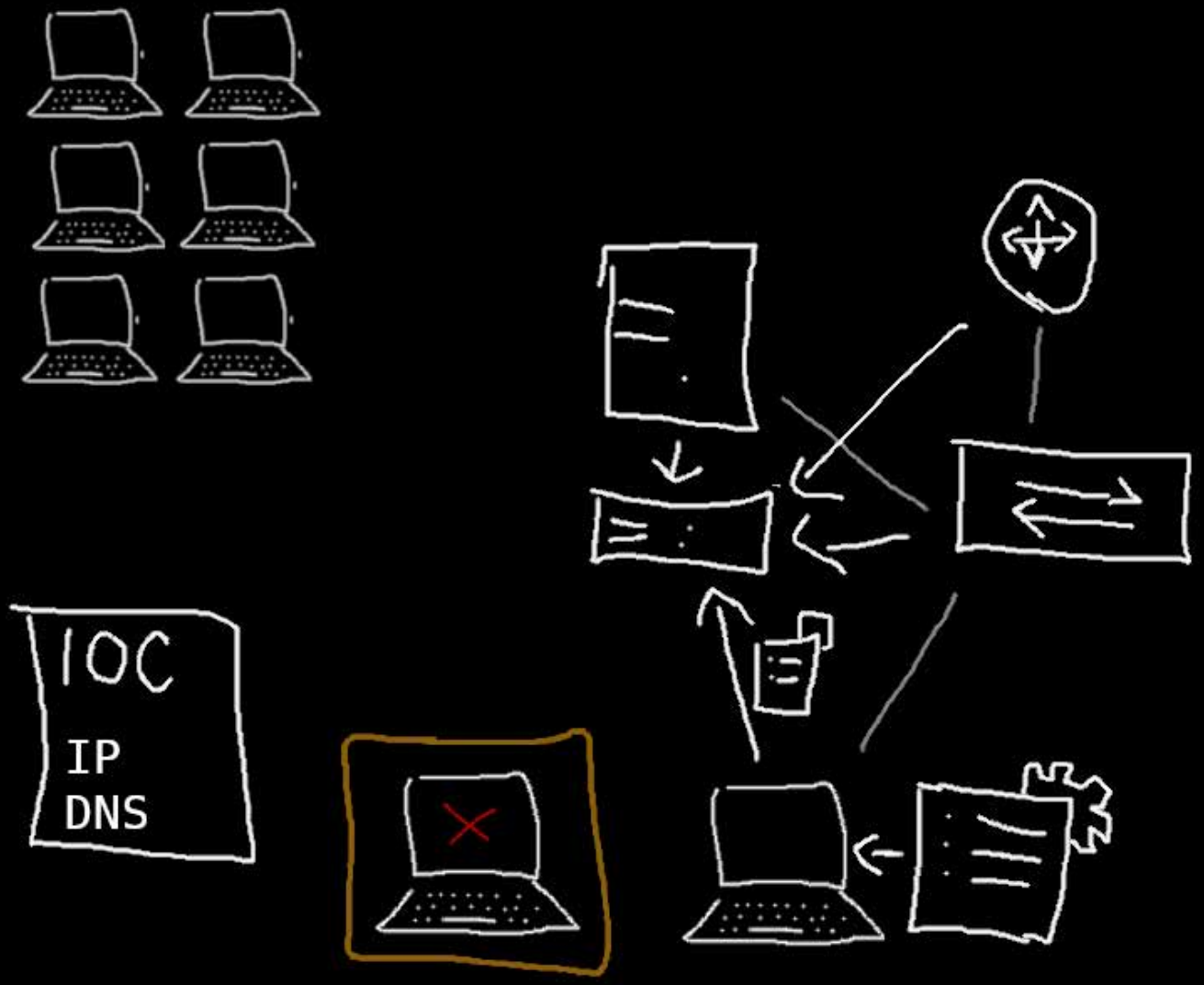
Incidents – Identifikācija -> ierobežošana



Identifikācija -> ierobežošana

- IP (Netflow, VPN, Firewall, IDS)
- DNS
- Citas iekārtas
- Digitālās analīzes rezultāti

Incidents – Identifikācija -> ierobežošana



Grūtības

- Nepietiekama tīkla plūsmas uzskaite
- Nav DNS pieprasījumu žurnalēšana
- Proxy IP adrese žurnālfailos
- Nepilnīgi sistēmas žurnālfaili

Atjaunošana

- Atjaunojam svaigu sistēmu
- Uzraugam, lai incidents atkal neatkārtojas

- **Grūtības:**
  - Nav ko atjaunot (rezerves kopijas)
  - Nav ar ko aizstāt (nav rezerves iekārtu)

Pēcanalīze

- Mācība no pieredzes
- Reālās darbības, lai incidents neatkārtojas

- Sagatavošanās nākamajam incidentam

CERT.LV

Paldies!

@cert.lv