Kiberdrošības draudu medības

CERT.LV pakalpojums

17/03/2026
Seminārs «Esi drošs»

Rūdolfs Ķelle

CERT.LV
Kiberincidentu novēršanas institūcija

Kas ir (un nav) draudu medības

- Draudu medības **ir** visu IT iekārtu analīze ar mērķi atrast:
    1) Aktīvu uzbrucēju klātbūtni
    2) Vēsturisku uzbrucēju klātbūtni
    3) Infrastruktūras vājos punktus
- Draudu medības **ir** CERT.LV servera nogāde, aģentu instalācija, aktīva komunikācija, dalīšanās ar atradumiem un ieteikumiem
- Draudu medības **ir** caurspīdīgs process – iespēja sekot līdzi mūsu darbam.
- Draudu medības **nav** "datu" apstrāde – netiek apskatīti dokumenti / prezentācijas / cits saturs.
- Draudu medības **nav** dienas aizsardzības pakalpojums (SOC)

Draudu medību process

1) **Sagatavošanās fāze**
   - Komunikācijas kanāla izveide (Mattermost)
   - CERT.LV servera nogāde
   - Draudu medību aģentu izplatīšana

2) Aktīvā fāze
   - Datu ievākšana un apstrāde
   - Saziņa, jautājumi par atradumiem (pēc nepieciešamības)
   - Reaģēšana uz incidentiem

3) Beigu fāze
   - Atskaites gatavošana, nodošana
   - Papildus datu ievākšana (pēc nepieciešamības)

Draudu medību process

Sagatavošanās fāze

Gatavs medībām!

- Komunikācijas kanāla izveide (Mattermost)
- CERT.LV servera nogāde
- Draudu medību aģentu izplatīšana

Aktīvā fāze

vairāki mēneši draudu medības

- Datu ievākšana un apstrāde
- Saziņa, jautājumi par atradumiem (pēc nepieciešamības)
- Reaģēšana uz incidentiem

Beigu fāze

Draudu medības pabeigtas

- Atskaites gatavošana, nodošana
- Papildus datu ievākšana (pēc nepieciešamības)

Draudu medības ieteicams atkārtot regulāri!

CERT.LV

Paldies!