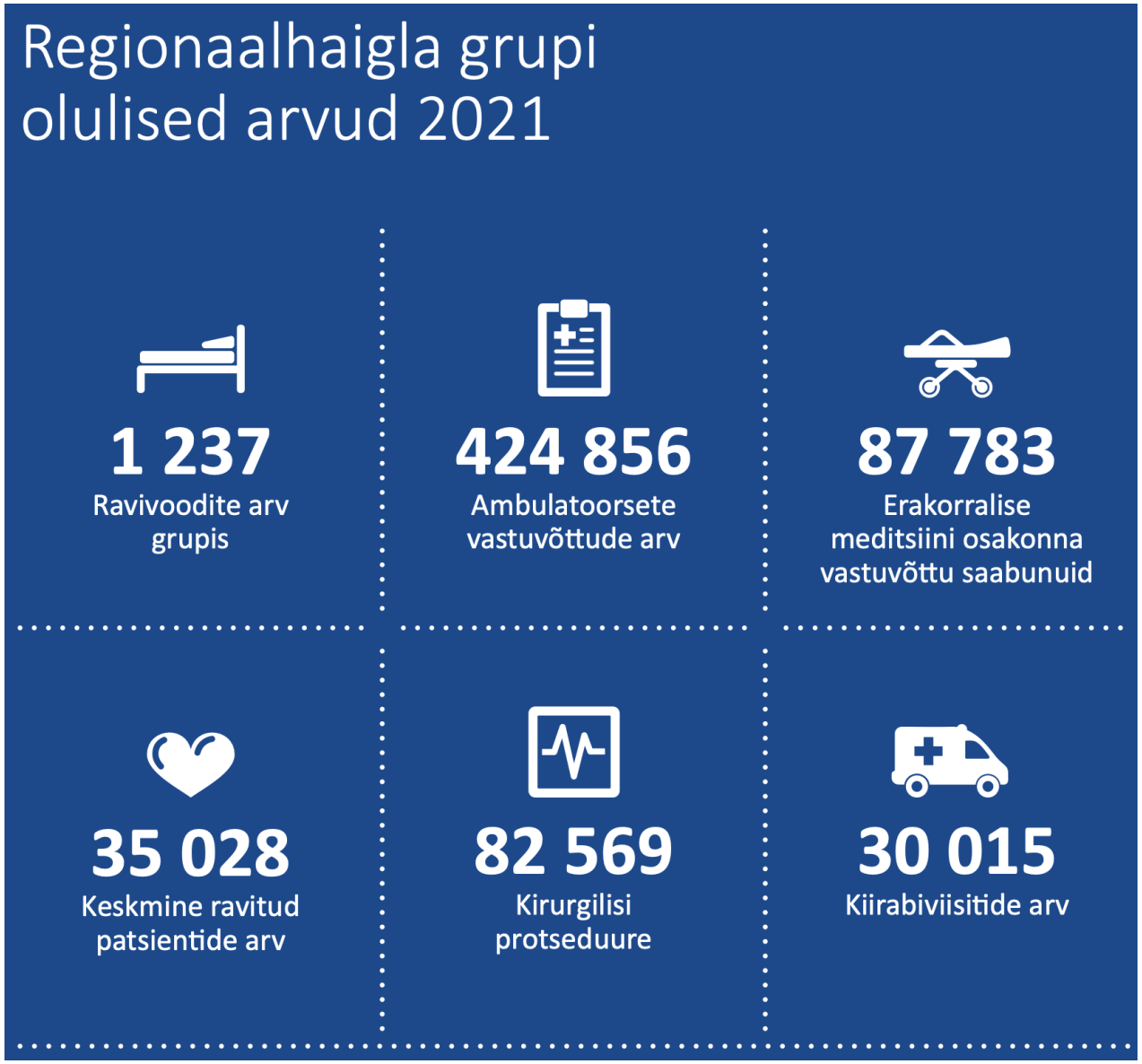
Regionaalhaigla

# Õppus „Küberreserv“ Regionaalhaiglas

Kristjan Hinn
Infoturbejuht

9. märts 2023

# Regionaalhaigla grupi olulised arvud 2021



# Küberõppused Regionaalhaiglas

- ENISA Cyber Europe 2022
- RIA Küberreserv 2022

Regionaalhaigla

RIIGI INFOSÜSTEEMI AMET

RIK
Registrite ja Infosüsteemide Keskus

TEHIK

RMIT
Rahandusministeeriumi Infotehnoloogiakeskus

smit

RIIGI INFO- JA KOMMUNIKATSIOONITEHNOLOOGIA KESKUS

KeMIT
11111011101

KAITSELIIT

certee

CR14

# Õppuse stsenaarium

Rünnak sai alguse uuest töötajast, kes täitis talle helistanud “tugiisiku” Jekaterina Russalkina korraldusi, käivitades arvutis pahavaralise tarkvara.

Rünnak levis algselt 3 arvutis, kuid peagi käivitus teine laine, mille tulemusel krüpteeriti kõik haigla arvutid.

Lisaks kürpteeriti ka kõik virtualiseerimiskeskkonna serverid koos neid teenindavate peaserveritega.

Tagatipuks oli IT teenistust tabanud NOVID viiruse laine, mille tõttu IT oli küll töövõimeline, kuid vähendatud koosseisus.

Regionaalhaigla

*Center Hospitalier Sud Francilien*

Home > News > Security > French hospital hit by $10M ransomware attack, sends patients elsewhere

# French hospital hit by $10M ransomware attack, sends patients elsewhere

By Bill Toulas

The Center Hospitalier Sud Francilien (CHSF), a 1000-bed hospit

August 23, 2022 12:23 PM 2

# LockBit Publishes Stolen Data as Hospital Rejects Extortion

French Government Vows Resistance, Stepped-Up Cybersecurity Funding

Mihir Bagwe (MihirBagwe) • September 26, 2022

Twitter Facebook LinkedIn Credit Eligible Get Permission

The Centre Hospitalier Sud Francilien (Image: Poudou99/CC BY-SA 3.0)

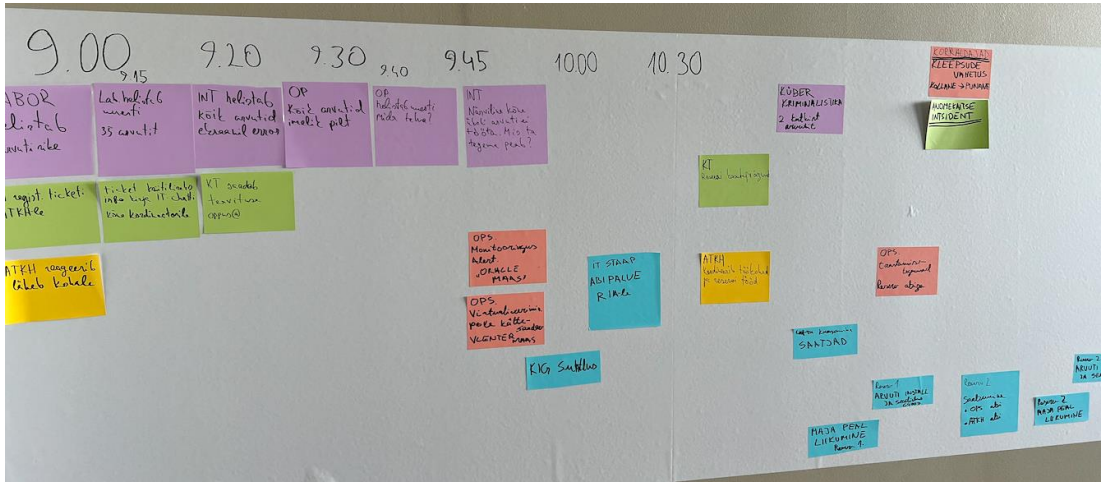
RESOURCES

OnDemand | API Protection – The Strategy of Protecting Your APIs

Live Webinar | Why

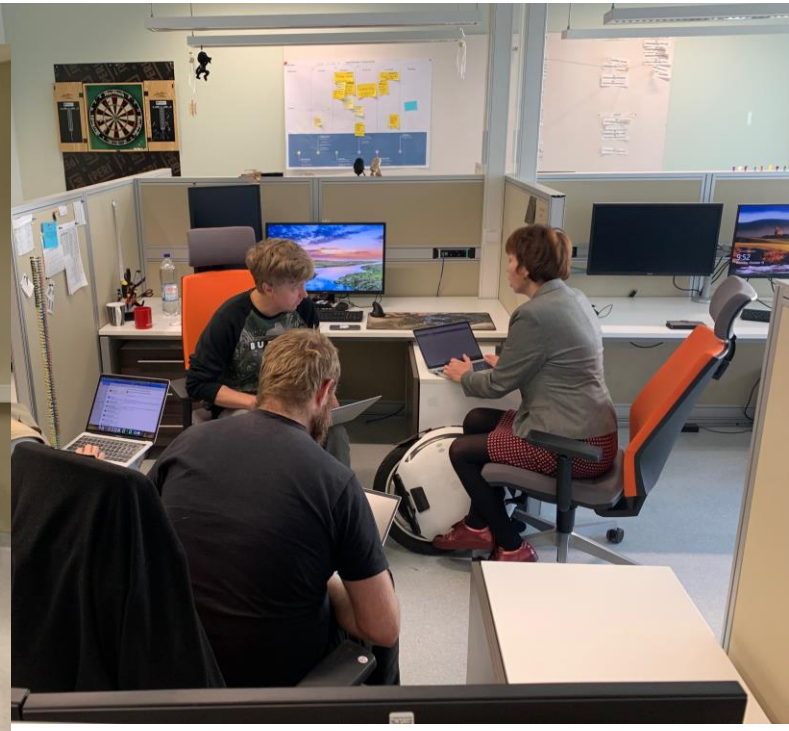
# Õppuse käik

- Intsidentide laekumine algas kell 9:00
  - Laboratoorium - kell 9:00, 9:15
  - Intensiivravi osakond II - kell 9:20
  - Operatsioonikeskus - kell 9:30, 9:45
- Serverite intsidendid - kell 9:45
- Küberreserv II taseme saabumine - kell 10:30
- Küberreserv III taseme saabumine - kell 13:00



# Kolm peamist probleemi, mida lahendada

- Taasteplaanide toimimine - Kuidas ja kuhu taastada serverid?
- Personalikriis - Meil pole piisavalt inimesi, et nakatunud arvuteid kiiresti välja vahetada.
- Digikriminalistika - Kuidas rünnak alguse sai? Tõendite kogumine.



# Peamised õppetunnid

- **Appi tõttav seltskond vajab juhtimist.**
- Küberreservi üksused peavad võimalikult autonoomselt hakkama saama.
- Kommunikatsiooni ahelad paika.
- Infovahetus standardiseerida.
- Praktika, praktika, praktika.

# Tänan!