Ankstyvo perspėjimo apie grėsmes paslauga

PROJEKTO VEIKLA 2.2.1

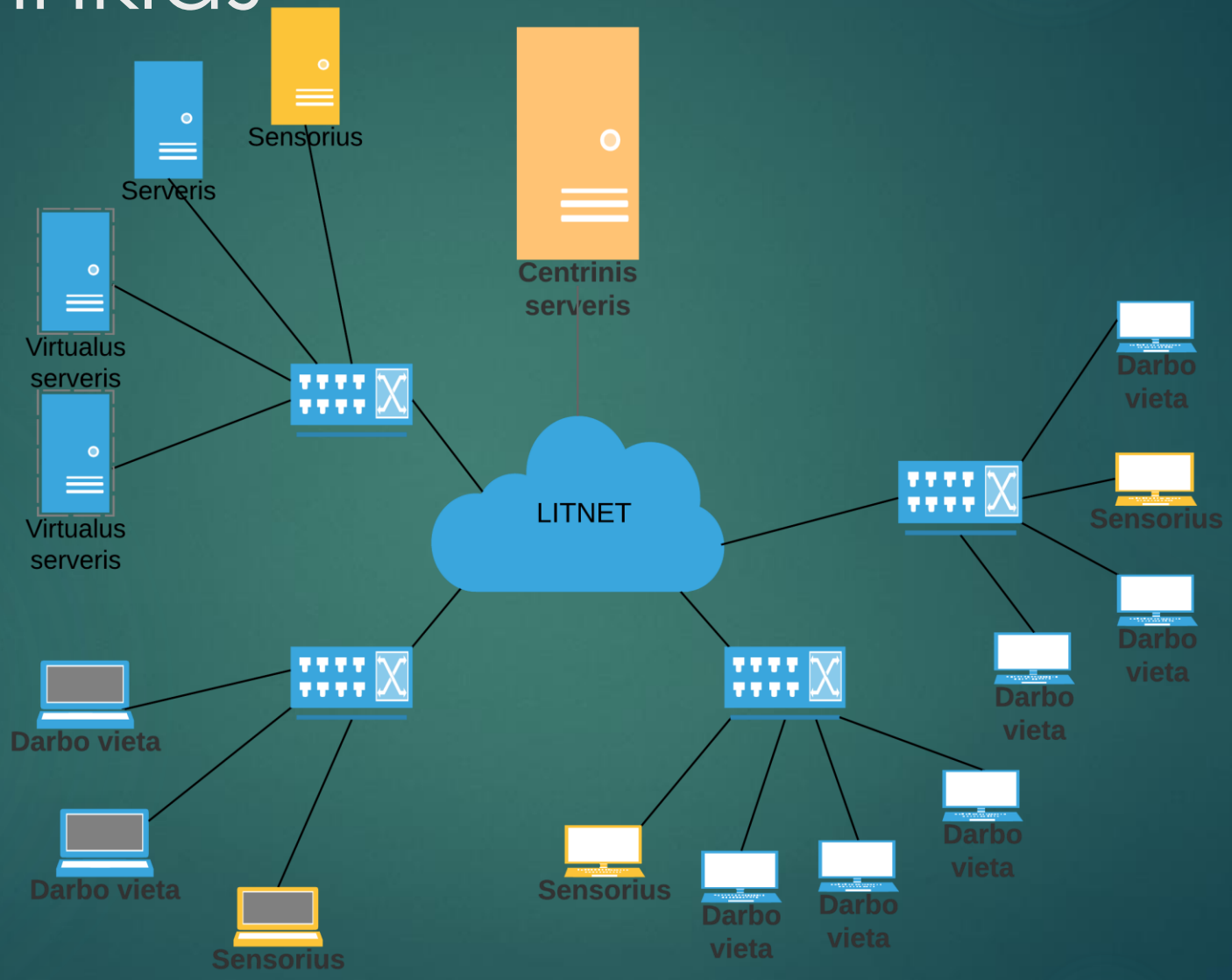
VALDAS PAŠKEVIČIUS

VU ITTC

Tikslai

- Sukurti centralizuotą sensorių tinklą naudojant pigius mikrokompiuterius
- Sukurti paprastą naujų sensorių prijungimo ir valdymo mechanizmą
- Rinki informaciją apie atakas nukreiptas į LITNET tinklo darbo vietas ir serverius
- Rinkti duomenis apie dažniausius atakų tipus, bandomus atspėti prisijungimo duomenis
- Automatiškai blokuoti atakuotojus pagal nustatytas taisykles
- Perduoti informaciją apie kenkėjišką veiklą tinkle vietiniams administratoriams

Sensorių tinklas



Sistemos veikimas

- Medaus puodynės (Honeypot) ir IDS programinė įranga
- Centralizuotas valdymas iš centrinio serverio per tinklalapį
  - Įrašai apie atakas
  - Statistika
  - Rankinis blokavimas ir baltasis sąrašas
  - Sensorių parametrų keitimas

Artimiausi planai

- Prisijungimas per SSO
- Pritaikymas naudoti automatinėse blokavimo sistemose
- Kitas pageidaujamas funcionalumas

Ačiū už dėmesį

- Pagaidavimai ir klausimai: valdas.paskevicius@ittc.vu.lt