DNS drošības analīzes un apziņošanas sistēma

Haralds Ķempelis

Māris Broks

Miks Lapsa

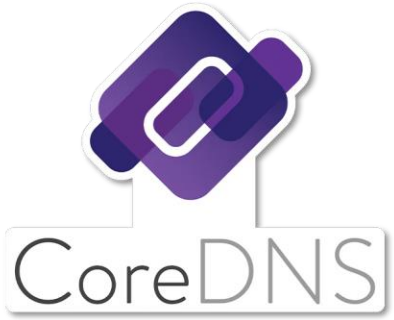
Egija Kokoreviča

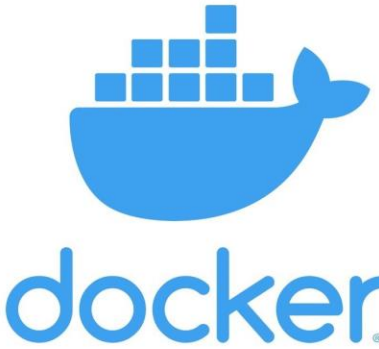
21.05.2025

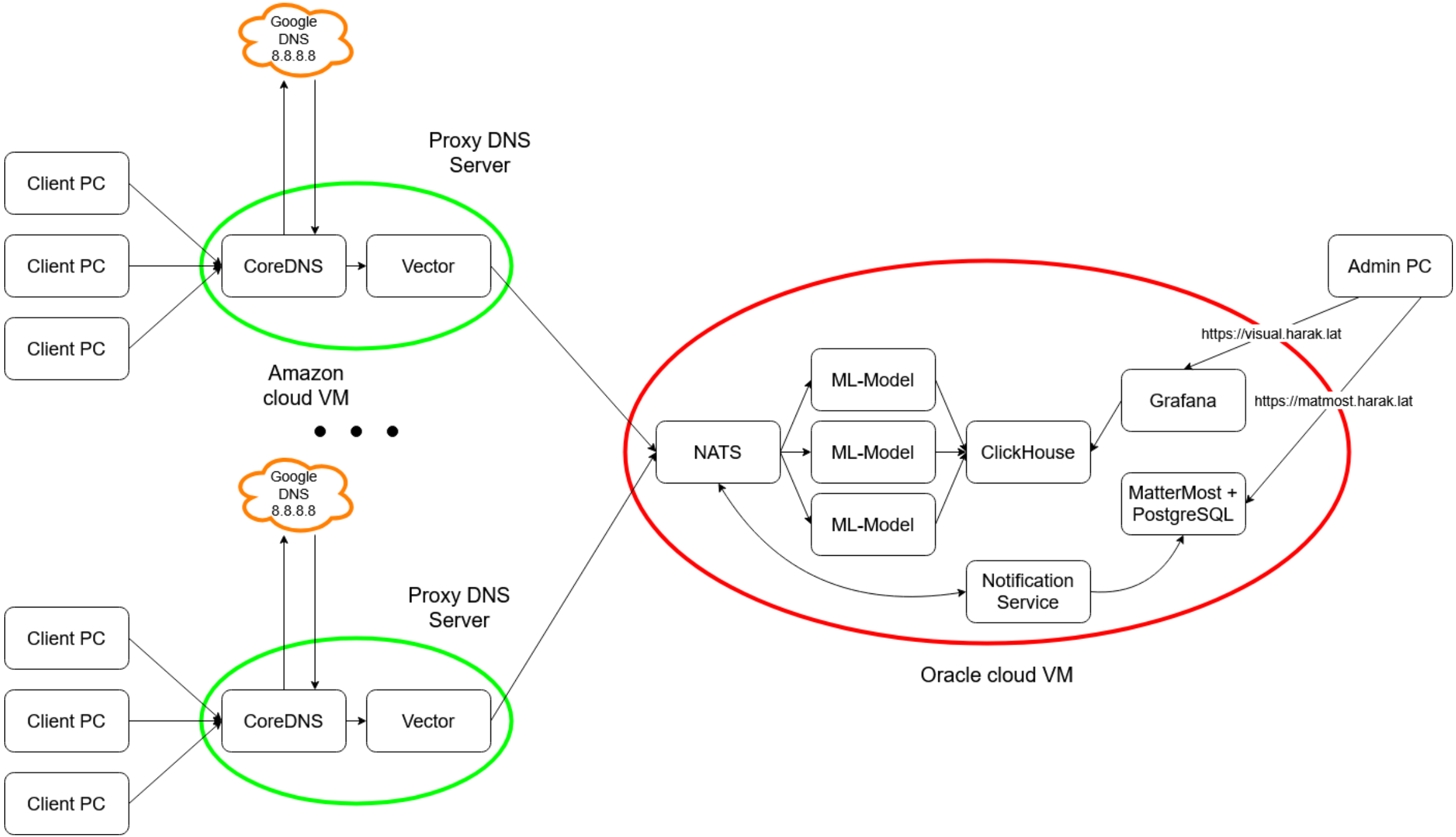
Uzdevums

- Izveidot risinājumu DNS logu analīzei, izmantojot mašīnmācīšanās modeli aizdomīgu adrešu filtrēšanai, integrējot Mattermost API apziņošanai un vizualizējot rezultātus interaktīvā infopanelī.
- Vizualizācija: https://visual.harak.lat/login (login: admgf499, password: SuperDrosalietotajaparole3!)
- Mattermost: https://matmost.harak.lat/login (login: admin, password: SuperDrosaMattermostParole!

Tehnoloģiju steks






Google
DNS
8.8.8.8
Proxy DNS
Server
Client PC
Client PC
Client PC
CoreDNS
Vector
Amazon
cloud VM
Google
DNS
8.8.8.8
Proxy DNS
Server
Client PC
Client PC
Client PC
CoreDNS
Vector
Admin PC
https://visual.harak.lat
https://matmost.harak.lat
ML-Model
ML-Model
ML-Model
NATS
ClickHouse
Grafana
MatterMost +
PostgreSQL
Notification
Service
Oracle cloud VM

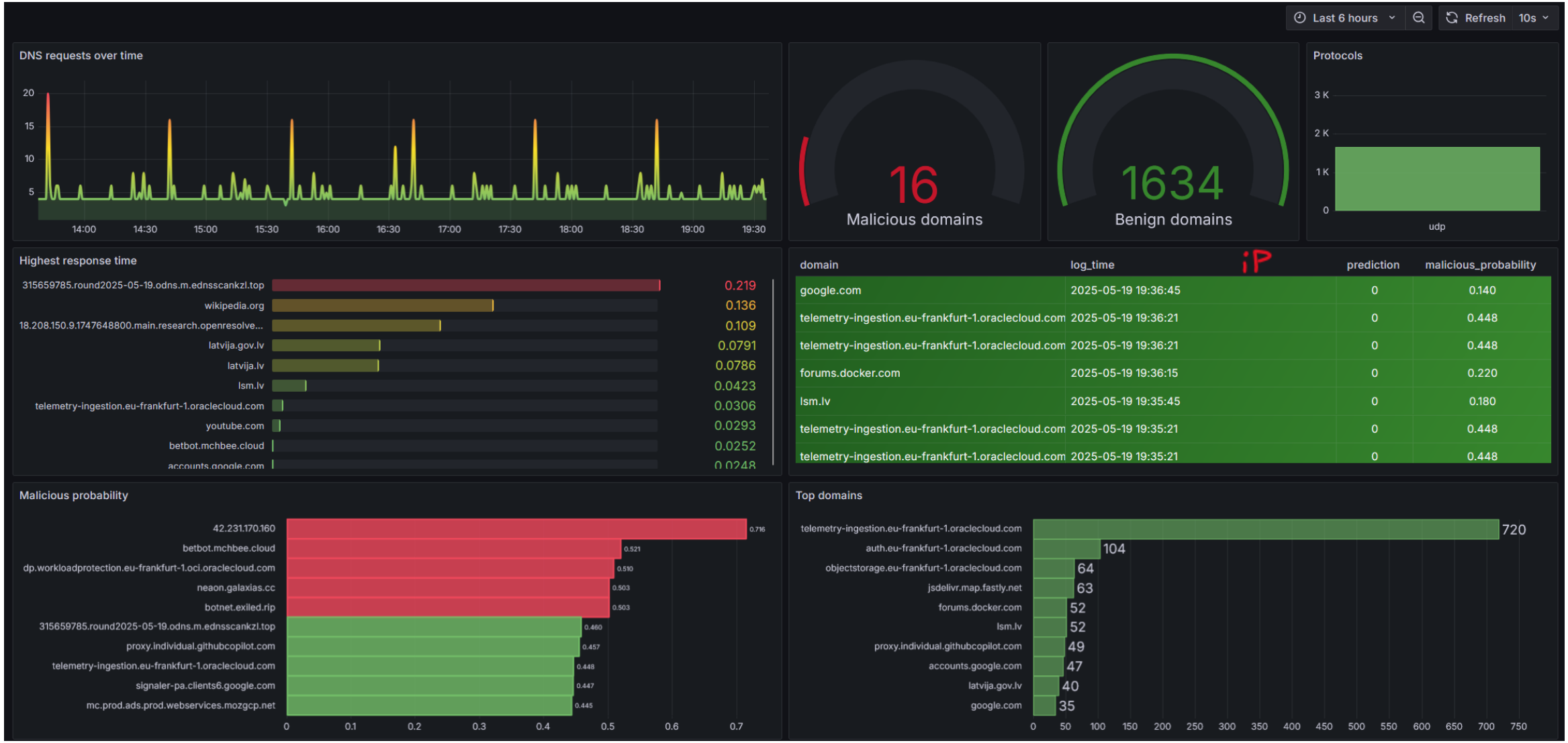
DNS ierakstu klasificēšana

- Mašīnmācīšanās pieeja - Gadījuma mežs (RandomForestClassifier)
- Pašu apkopota datu kopa (Tranco list, urlhaus.abuse.ch, u.c)
- Vairāki atribūti no DNS loga, kas raksturo pieprasījumu (domēna garums, pieprasījuma tips, u.c.)
- Binārās klasifikācijas uzdevums – 0 nav ļaunprātīgs, 1- ir ļaunprātīgs
- Ir whitelist/blacklist funkcionāls

Mattermost

- Automātiska komandas, kanāla, webhook izveide ar mmctl
- Ziņojumi nodrošināti ar Webhook palīdzību

Vizualizācijas (Grafana)



Paldies par uzmanību!