Ankstyvo perspėjimo apie grėsmes sistema

VALDAS PAŠKEVIČIUS

VILNIAUS UNIVERSITETAS

2018

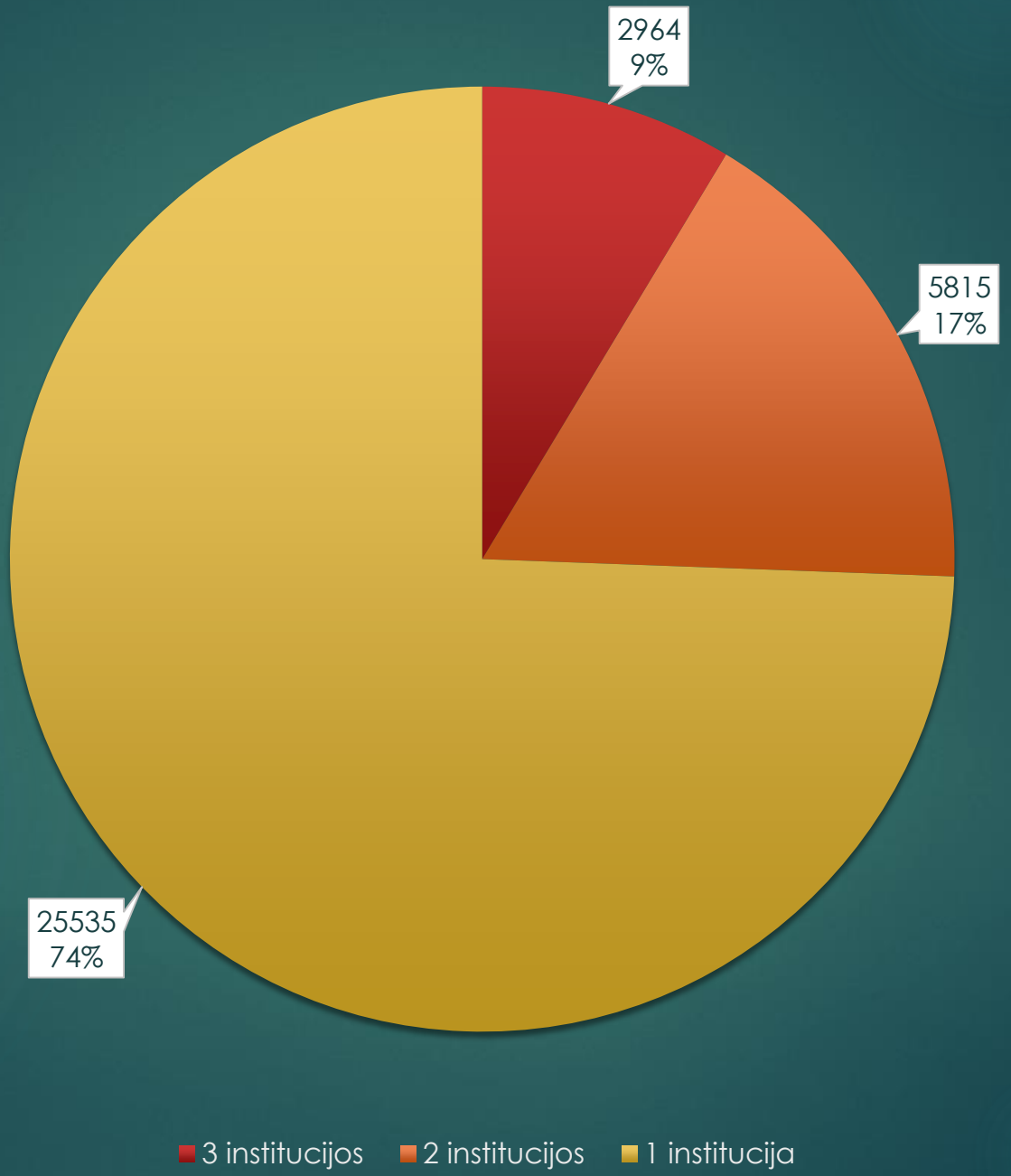
Tikslai

- Informacijos apie atakas rinkimas
- Pokyčių stebėjimas
- Informavimas
- Atakų prevencija

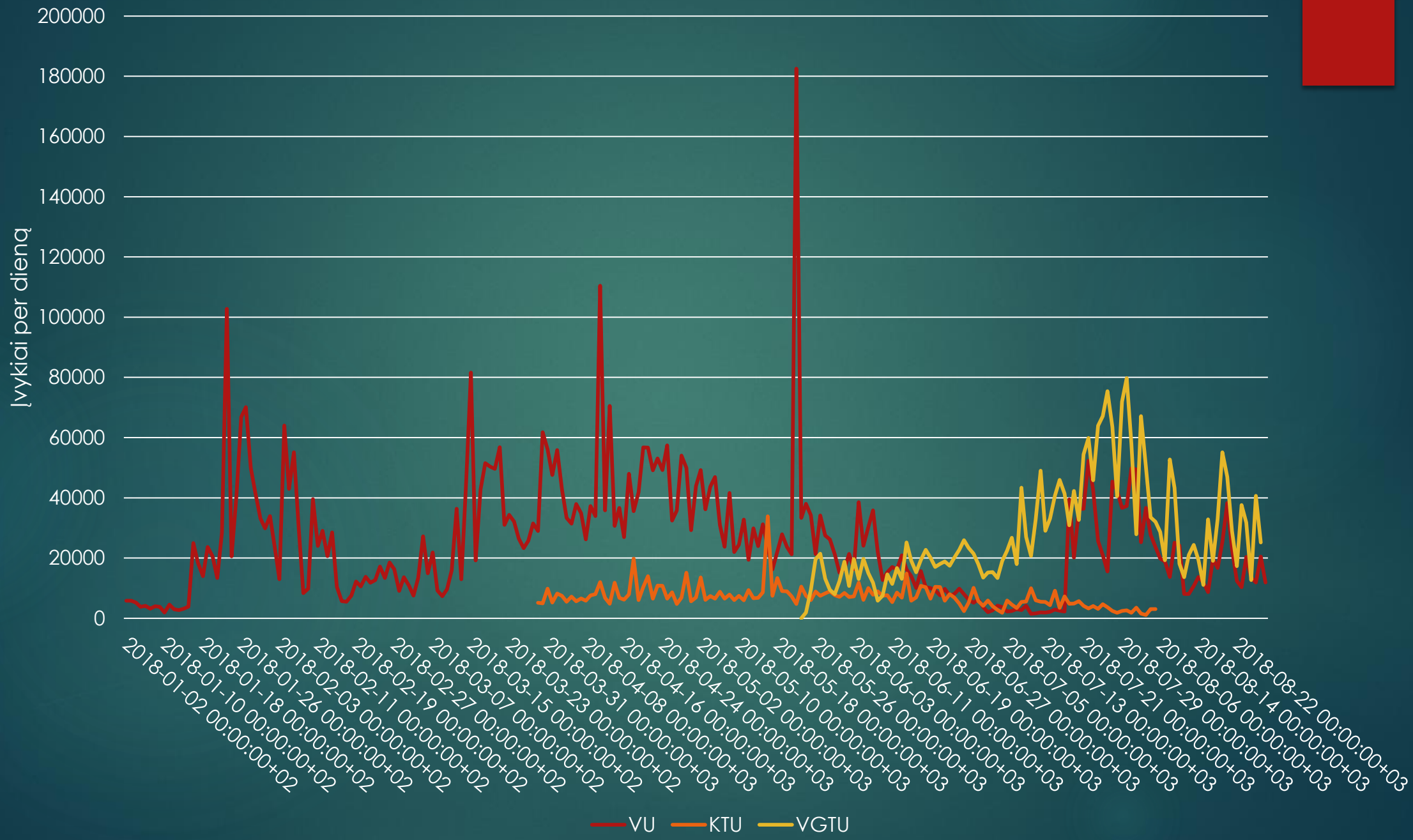
Renkama informacija

- Portų skenavimai
- Prisijungimo bandymų duomenys
- IDS informacija

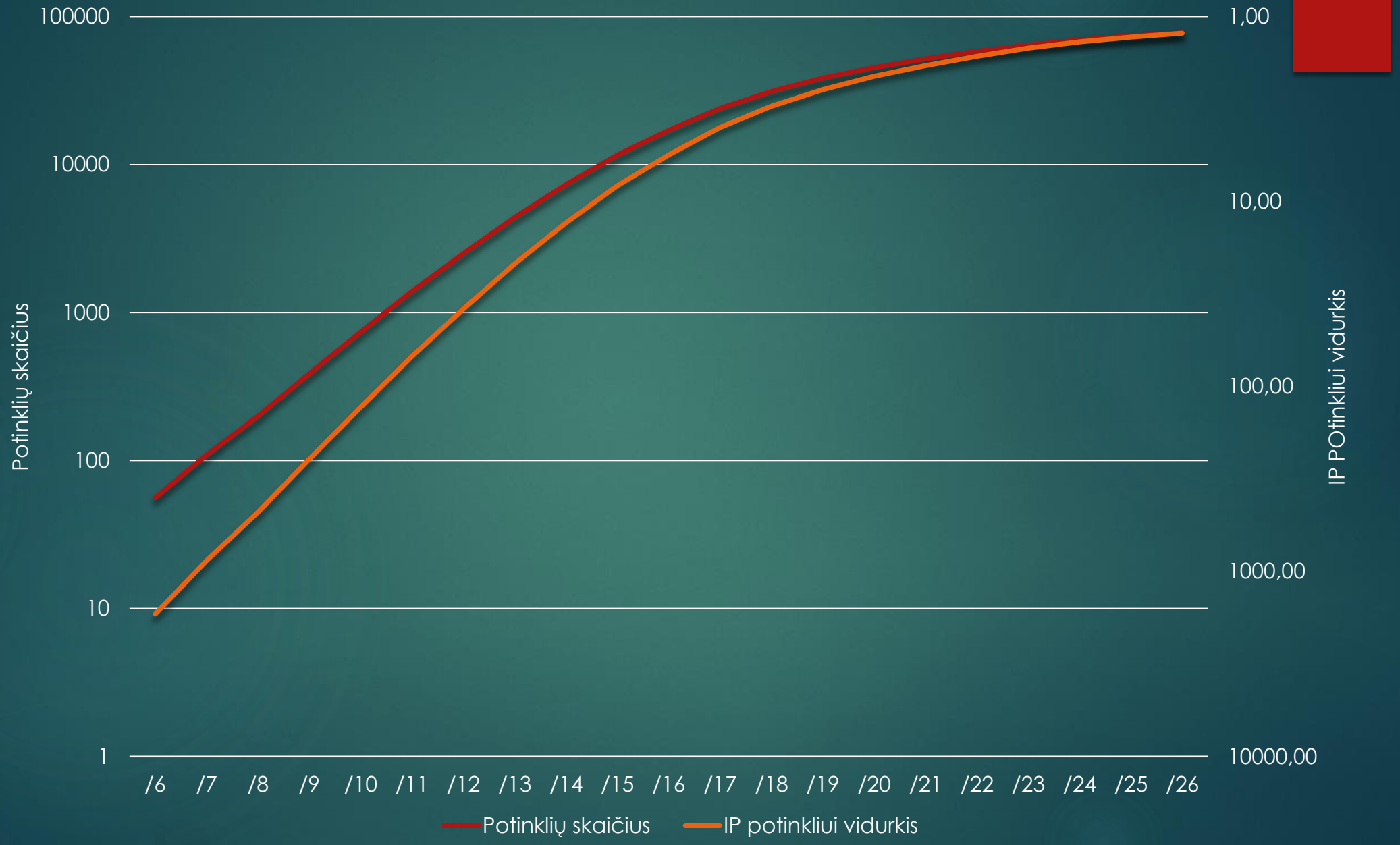
Užfiksuoti IP skirtingų institucijų sensoriuose (nuo 2018-06)



Įvykiai per dieną pagal institucijas (užsienis)



Pažeidėjų pagal potinklius statistika



Top 20 skenavimų LT

Portai	Kiekis
Scan: tcp 139-445	128283
Scan: udp 137	97065
Scan: udp 161	43780
Scan: tcp 445	17021
Scan: tcp 139	13006
Scan: tcp 8291	6748
Scan: tcp 7547	6007
Scan: tcp 23	5454
Scan: tcp 443	2996
Scan: tcp 10050	2853
Scan: icmp	2394
Scan: udp 53	216
Scan: tcp 8080	204
Scan: tcp 443-10050	158
Scan: tcp 5555	155
Scan: udp 389	152
Scan: tcp 8000	117
Scan: tcp 9981	109
Scan: tcp 8888	101
Scan: udp 45769	92

Top 20 įvykių tipų (IDS duomenys) LT

Tipas	Kiekis
ICMP Destination Unreachable Communication Administratively Prohibited	4264074
SNMP trap udp	714841
SNMP request udp	151133
ICMP PING	134658
SNMP public access udp	129166
SCAN UPnP service discover attempt	93557
ICMP Destination Unreachable Host Unreachable	62003
ICMP L3retriever Ping	25061
ICMP PING *NIX	19544
MISC UPnP malformed advertisement	14164
HoneyPotSSHTransport	9040
ICMP Destination Unreachable Port Unreachable	7691
Honeypot httpd	6819
SNMP missing community string attempt	5397
NETBIOS name query overflow attempt UDP	1085
DNS SPOOF query response with TTL of 1 min. and no authority	980
ICMP Echo Reply	689
RPC portmap proxy attempt UDP	674
DNS named version attempt	435
SNMP request tcp	359

APGS naudotojo aplinka

- Sensorių valdymas
- Paskutinių įvykių stebėjimas
- Statistika
- Pažeidėjų statistika
- Baltieji/institucijų potinkliai
- Taisyklių pažeidėjams aprašymas

Planai

- Integracija su blokavimo sistemomis (užkardos ir kt.)
- Tikslinės informacijos rinkimas
- Informacijos analizavimas

Ačiū už dėmesį

Klausimai, pageidavimai:
litnet@tinklas.vu.lt