SECURITY DAYS

NATO VIRŠŪNIŲ SUSITIKIMAS. KAIP TAPTI NEĮVEIKIAMA INTERNETO TVIRTOVE: „TELIA LIETUVA“ ATVEJIS

Andrius Šemeškevičius - Telia Lietuva
technologijų vadovas

Rugsėjo 5 d. 2024
KIBERNETINIO SAUGUMO KONFERENCIJA
esd.eset.lt

Reikalavimų puslapiai ir terminai

41

psl. sutartis

Reikalavimų puslapiai ir terminai

29

psl. sutarties priedų

Reikalavimų puslapiai ir terminai

+89

psl. NATO techninių reikalavimų rinkinys

Reikalavimų puslapiai ir terminai

Sprendimo apimtys

Ryšių sprendimas

Kompiuterinių tinklų įrengimas ir priežiūra

Saugumas

Darbo vietos ir jų priežiūra

Dokumentų spausdinimas ir naikinimas

Military grade

Petras Malukas | AFP | Getty Images

Pasiruošimas

Įrangos užsakymas, rezervo formavimas

1

Viso Telia tinklo perimetro apsaugos stiprinimas - papildomos kelių lygių apsaugos priemonės, tokios kaip anti-DDoS, WAF

2

Papildomas „slaptas“ išėjimas į pasaulinį internetą

3

Aukščiausių saugumo priemonių pritaikymas Litexpo/NATO tinklų sprendime

4

Testavimai ir skenavimai tiek iš išorės, tiek ir iš vidaus

5

Įsilaužėlių forumų ir Telegram grupių stebėjimas

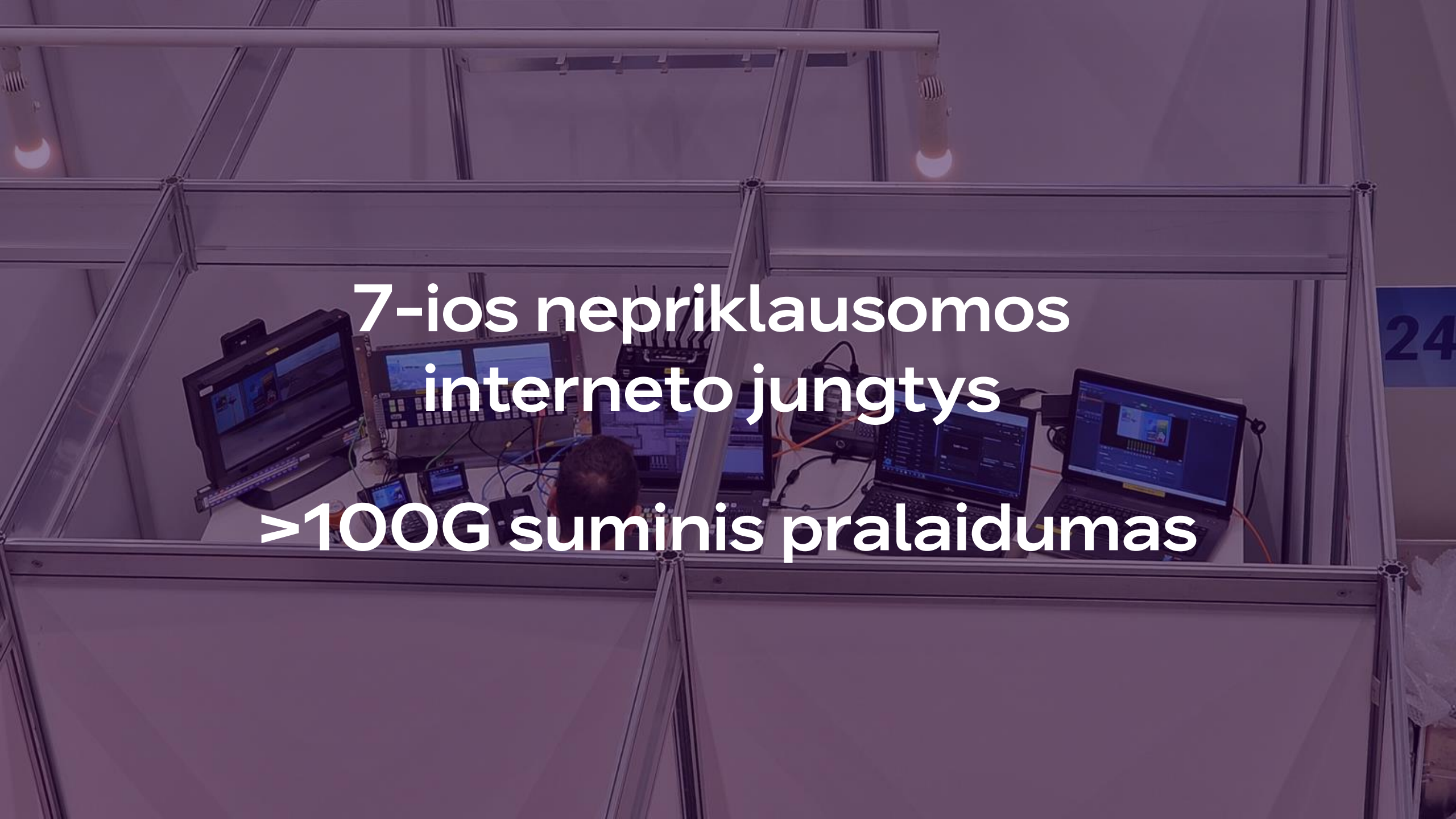
6


> 2000
darbo vietų

> 5000
unikalių vartotojų


> 3500 vienu metu
dirbančių įrenginių

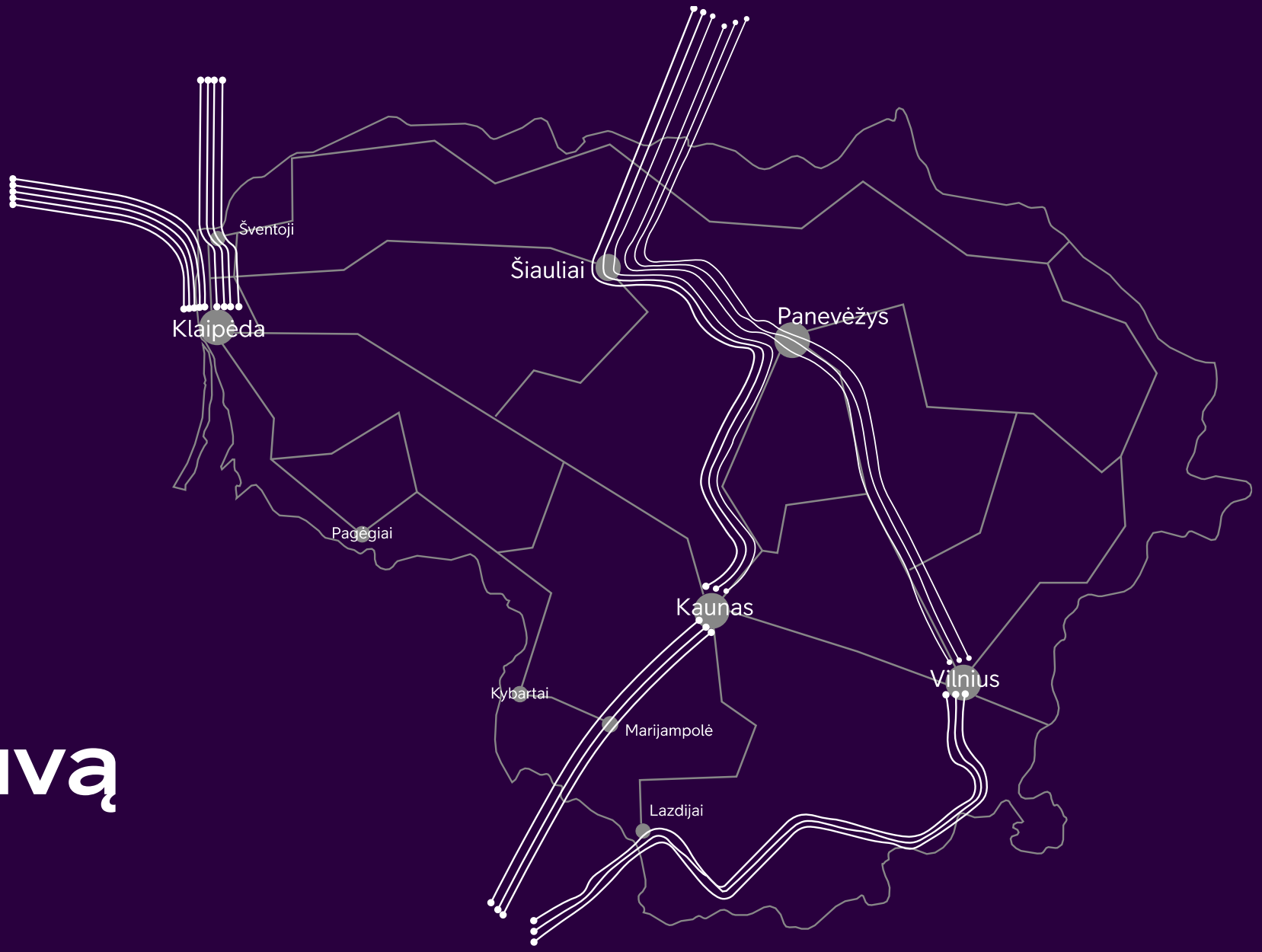

6 fizinės ugniasienės,
109 WiFi AP



7-ios nepriklausomos interneto jungtys

>100G suminis pralaidumas

Interneto keliai į Lietuvą




150 km LAN kabelių
60 LAN komutatorių


10 km optinio kabelio
1500 optinių gijų

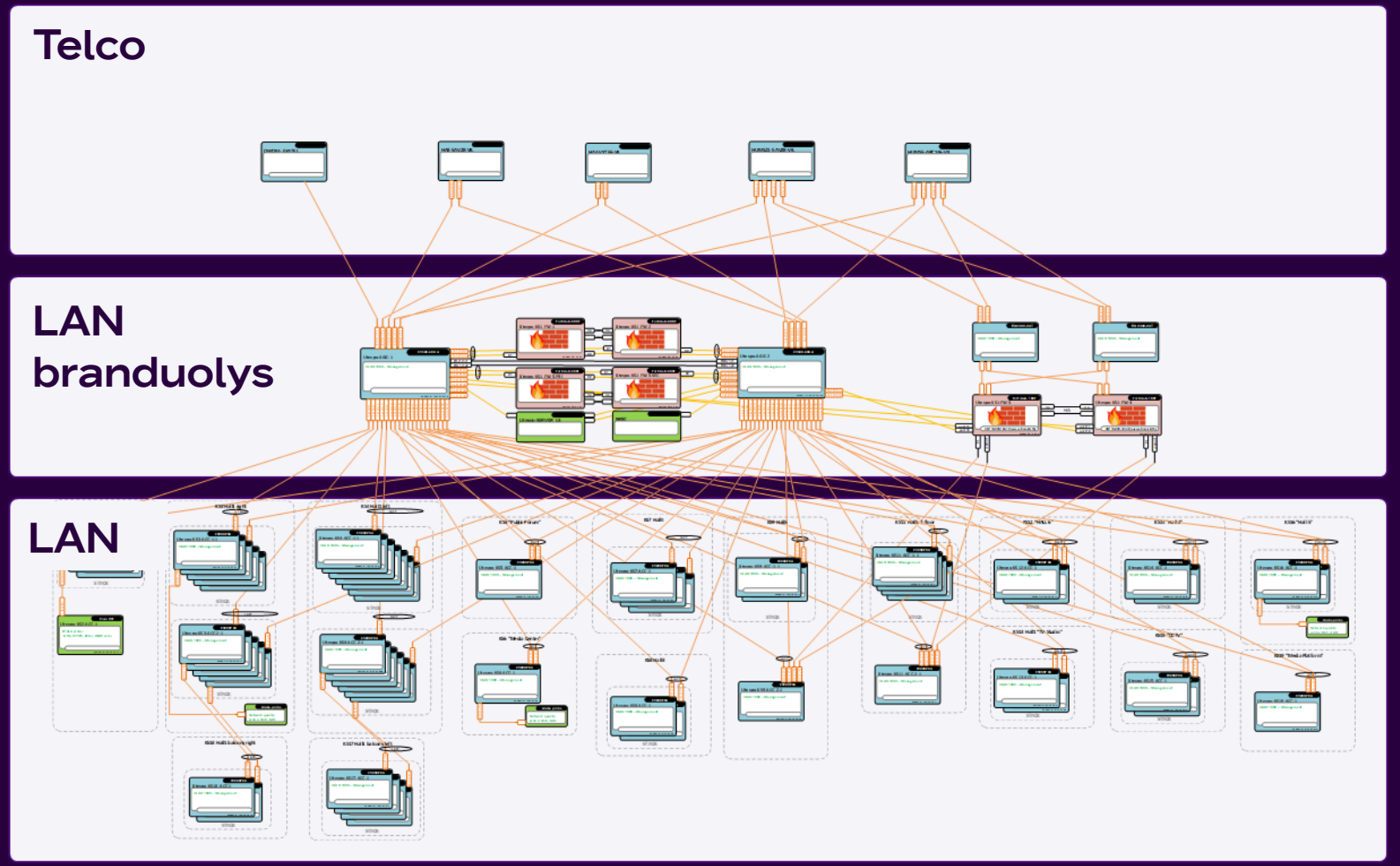
Dedikuotas DNS sprendimas su NKSC integracija

Pagrindiniai servisai Litexpo (NATO) tinkle:

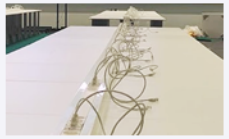
- Internet access
- TV contribution services
- TV distribution services
- CCTV
- VoIP telephony
- Printers
- Etc.

Tinklo architektūra sukurta, vadovaujantis šiais principais:

- Hi-Capacity
- Hi-Availability
- Hi-Security



Ethernet



1800
portų

WiFi

109
Didelės talpos AP

CORE | Ugniasienės ir LAN branduolys

Firewalls

Strictest NAT, without additional port-forwards and other types of exceptions

Monitoring to detect network anomalies:
- Inside the network – probing, spoofing, infections, etc.
- Outside network – abnormal DDoS like behaviors
- Advanced analytic tool for data analysis
- Advanced UTM security package

Telco access

- Shared/media internet 2 x N x 10 Gbps
- Dedicated internet N x 10 Gbps uplinks
- N x 10 Gbps uplink to special global internet provider
- 2 x 10G for management and secure internal communication

Switching core

- Hi-Bandwith 160G backplane
- Nx10G aggregation ports

For all network appliances

Completely isolated management – separate VDOMS, Mgmt. ports, comm. lines

ACCESS | Prieiga ir jos saugumo sprendimai

19
Access racks

22
Stacks

60
Switches

Cisco
C9200PXG
10G switches

Configured with extra strict security policy:

- IP spoofing detection and automatic prevention
- Rogue DHCP server injection detection and prevention
- ARP spoofing detection and automatic prevention
- Intra client isolation (private VLAN)
- Storm detection and automatic suspension
- VLAN hoping prevention
- BPDU guard, control packet injection prevention
- Control requests limiting

Anomalies detection and alerting:

- Traffic jams
- Loops and storm control
- All kinds of security events

General security philosophy:

- Automatic anomaly detection and suppression

WiFi | Didelio našumo WiFi

109
Access points

14
outdoor

95
indoor

Hi-Performance AP:

- Each capable to serve up to 1024 customers.
- Over 100k clients can be served in theory
- WiFi 6 (802.11ax)

Configured with moderate security – to balance between accessibility and security:

- NATO Press (SSID)
- NATO Summit (SSID)

Additional security features:

- ARP anti-spoofing
- ARP request rate limit 15 per min
- DHCP request rate limit 15 per min
- Wireless client isolation
- Radio bandwidth utilization control

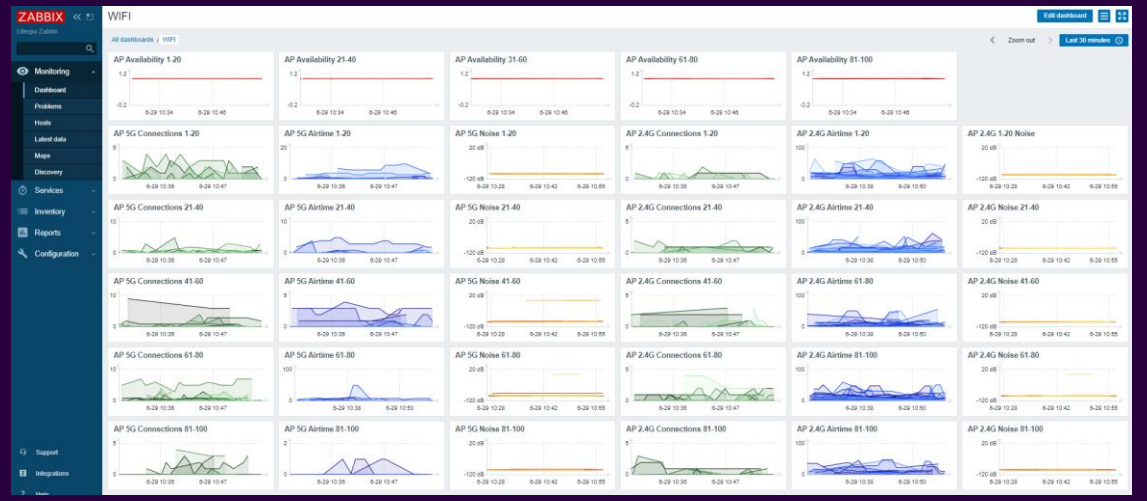
Anomalies detection and alerting:

- Rogue WiFi AP detection
- Abnormal Radio bandwidth utilization
- Heavy user detection
- Abnormal client behavior

NoC & SoC 24x7 | Vietinis tinklo valdymo ir saugumo centras

Monitoring:

- Alerts accumulation and sorting from all network appliances
- Performance metric pooling and charting
- Most important statistics correlating to sniggle view charts
- Advanced statistics gathering, such as:
  - Wired user experience simulating (wired probes) and monitoring
  - Wireless probes analyzing user experience
  - Radio frequency utilization statistics

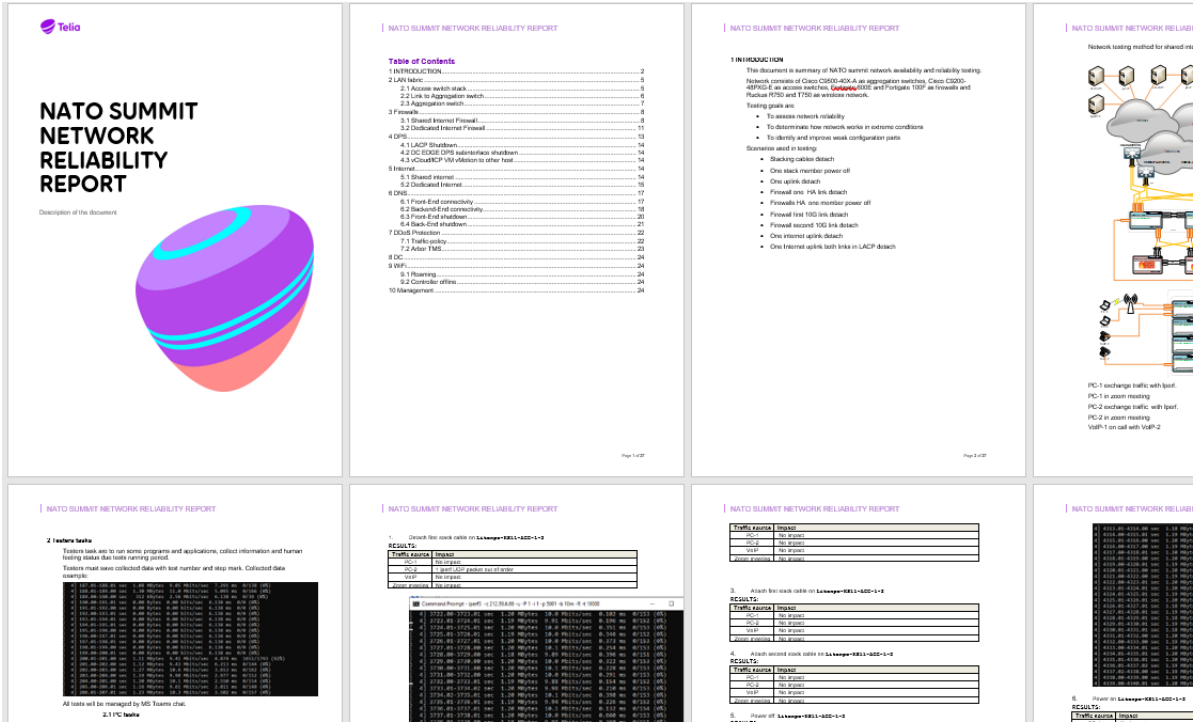


SOC level security analysis and tools:

- SIEM tool
- UTM deep inspection package in monitoring mode
- Packet capture and analysis on any point of network
- Syslog automatic sorting, highlights and manual review

Personalas ir darbo organizavimas 24x7

- Dedikuoti inžinieriai ir dar priskirti po 2 budintys kiekvienai sričiai
- Pasirengimas ir pratybos siekiant imituoti saugumo incidentus ir tinklo gedimus
- Atsarginės įrangos dalys ir apmokytas personalas
- Specifiniai susitarimai su specialiosiomis tarnybomis dėl saugos incidentų
- Telegram grupių ir įsilaužėlių forumų stebėjimas realiu laiku
- Organizaciniai procesai gedimų, saugumo incidentų ir krizės atveju
- Visos įmonės mobilizacija renginio periodui



Užkulisiai

Įsilaužėlių radaras

Зачем НАТОвцам мультимедийный портал? Вот и мы не знаем. Убрали.

❌https://check-host.net/check-report/10942691k82b

👉**Подписывайтесь на** канал NoName057(16)
🐻**Вступайте в наш** DDoS-проект
⚠️**Подписывайтесь на** резервный канал
🔻Eng version

🇷🇺**Победа Za нами!**

А знаете ли вы, где проходит сегодня саммит НАТО? В "Литэкспо", сайт которого мы положили с самого утра 😂😂

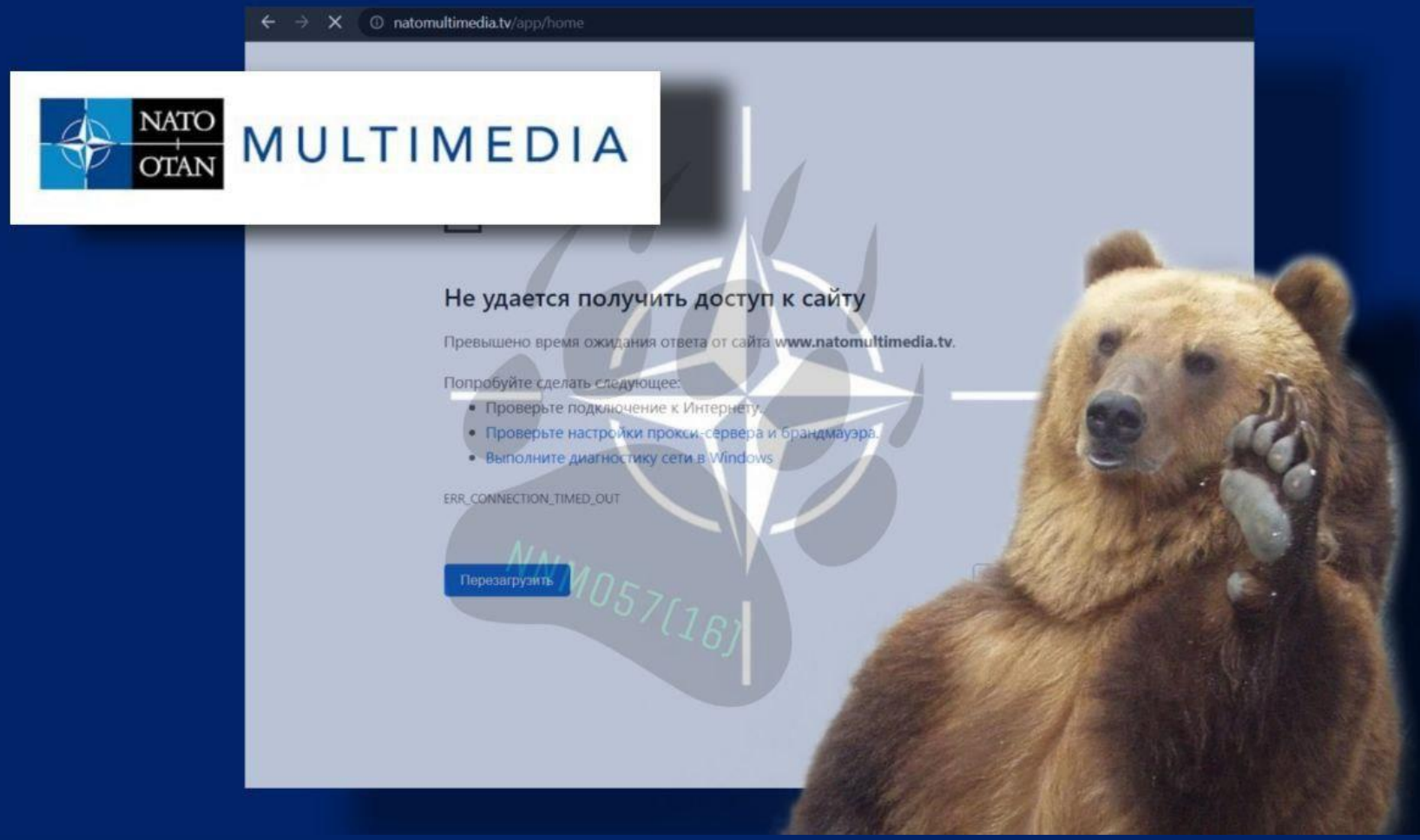
❌https://check-host.net/check-report/109423a9kc48

👉**Подписывайтесь на** канал NoName057(16)
🐻**Вступайте в наш** DDoS-проект
⚠️**Подписывайтесь на** резервный

Русофобские власти Литвы, которые не знают, как справиться с русскими хакерами из NoName057(16) предложили побыть своим гражданам терпилами😂

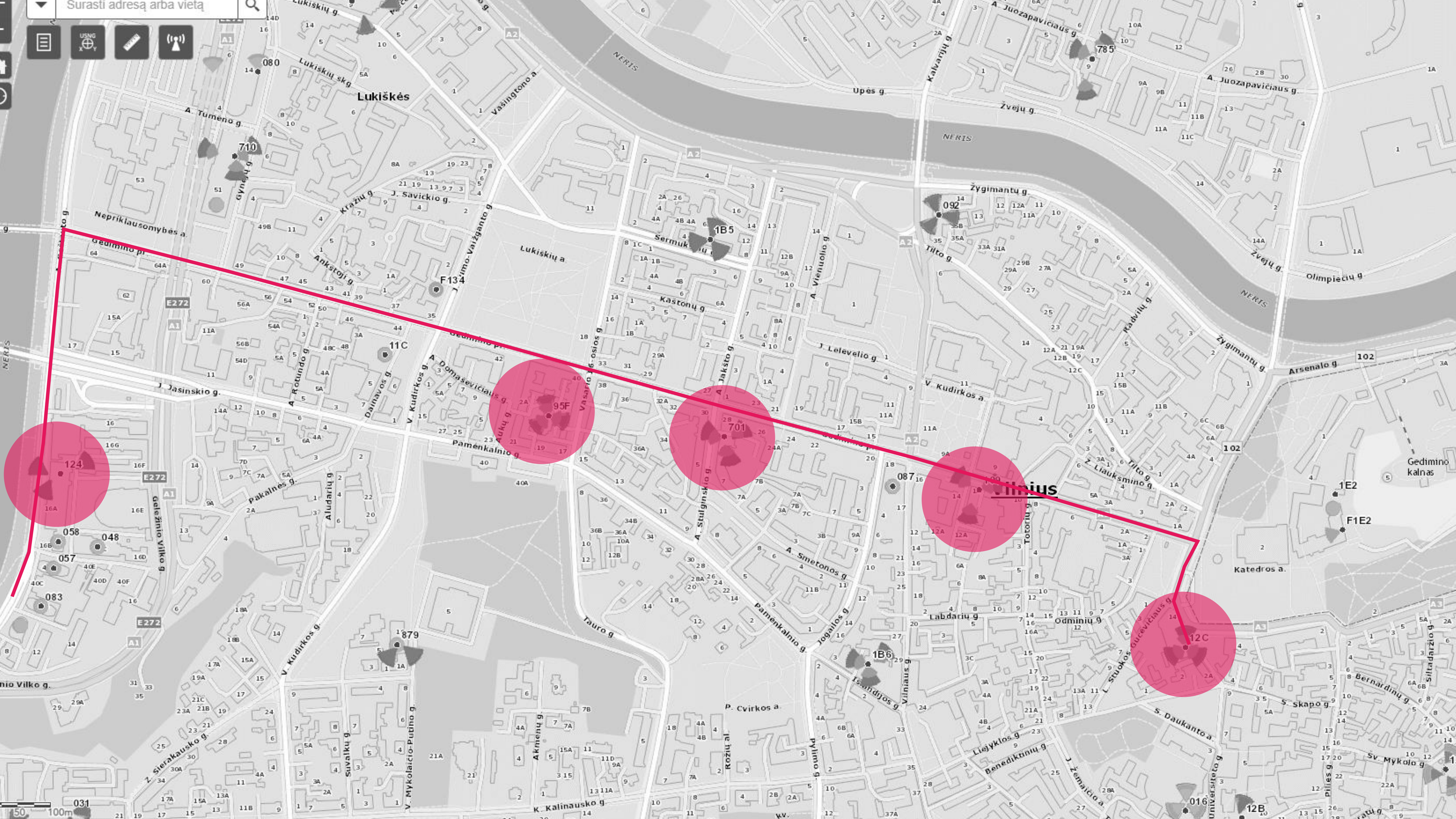
Второй день в Вильнюсе не

„Blogas“ internetas




CANADA

D. Umbraso nuotr.



Surasti adresą arba vietą
Lukiškės
Lukiškių a
Neris
Vilnius
Gedimino kalnas
Gedimino pr.
Nepriklausomybės a.
A. Tumeno g.
J. Jasinskio g.
Pamėnkalnio g.
A. Domaševičiaus g.
V. Kudirkos a.
J. Lelevelio g.
Žygimantų g.
Tilto g.
Arsenalo g.
Katedros a.
Odminių g.
Labdarių g.
S. Daukanto a.
Bernardinų g.
Liejyklos g.
Benediktinių g.
Islandijos g.
P. Cvirkos a.
K. Kalinausko g.
Geležinio Vilko g.
Pakalnės g.
Tauro g.
A. Smetonos g.
A. Stulginskio g.
Jogailos g.
Vilniaus g.
J. Savickio g.
Kražių g.
Upės g.
Žvejų g.
A. Juozapavičiaus g.
Olimpiečių g.
Kalvarijų g.
Vašingtono a.
Šermukšnių g.
Kaštonų g.
Vienuolio g.
Radvilų g.
Z. Liaukšmino g.
Totorių g.
Vasario 16-osios g.
Sv. Mykolo g.
S. Skapo g.
J. Žemaitės g.
Universiteto g.
Sierakausko g.
Aludarių g.
Rotundo g.
Dainavos g.
Mykolaičio-Putino g.
124
95F
701
12C
080
710
1B5
092
785
F134
11C
087
058
048
057
083
879
1B6
1E2
F1E2
102
016
12B
031

Projekto svarba padiktavo kitokį elgesį

Projekto svarba padiktavo kitokius sprendimus

CEO 2 CEO dėl tiekimo terminų

Internetui planas „C“ per slaptą tiekėją

Ryšio slopinimo iššūkiai

Fiksuotos telefonijos sprendimai

Incidentų testai, atakų imitacija

„Login 2023” pratybos

„Change Freeze“

Sprendimų estetika

Projekto svarba padiktavo „kitokią“ komandą

6 mėn. specialiųjų tarnybų patikra

Naktimis budi tik „senior“ lygio ekspertai

Dvigubi budėjimai

Dedikuota krizių valdymo komanda

„Telia“ grupės užnugaris

Bendradarbiavimas su policija

Saugos incidentų valdymas su specialiosiomis tarnybomis


Pamokos

Pavyko laikytis „10 saugumo įsakymų“

I
Apsauga nuo atakų „iš vidaus”

II
Apsauga nuo išorės atakų ir DDoS

III
„Cloud“ paslaugų valdymas

IV
„Web“ aplikacijų kūrimas ir atnaujinimas

V
Techninės įrangos atnaujinimas

VI
Programinės įrangos atnaujinimas

VII
Ryšių infrastruktūros atsparumas

VIII
Pasiruošimas Greitam veiklos atstatymui

IX
Krizių valdymas

X
Dedikuotas kibernetinio saugumo biudžetas

Teorijų klasika realybėje

Suvokta motyvacija vardan ko?

Sunku pratybose, lengva kare

Galima ir iš pirmo karto

Rizika paslysti „lygioje vietoje”

Reikėjo rezultato, o ne sutaupytų pinigų

Kai yra kontrolės mechanizmas

Kai devynis kartus pamatuoji, dešimtą kerpi

Ačiū