Tet IT Security

Never Forgets

Latvijas Pašvaldību savienība

Kiberdrošība pašvaldībās –

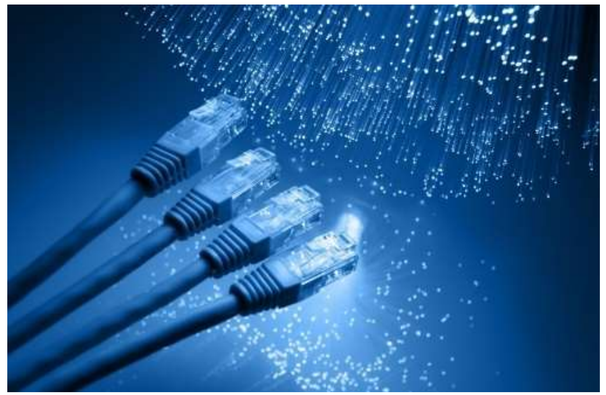
KĀPĒC tā ir tik **SVARĪGA**

Artūrs Filatovs
Kiberdrošības Eksperts

tet

Pakalpojumi valsts un privātajam sektoram

Nodrošinām 54% Latvijas interneta plūsmas



Savienojamība

Čatbots, 24/7 zvanu centri, pieteikumu sistēmas

AI Mākslīgais Intelekts

Apkalpojam vairāk kā 5800 darbstacijas un 2200 serverus

Datoru apkalpošana un speciālistu īre

Pakalpojumi valsts un privātajam sektoram

5 datu centri Latvijā (ISO27001, PCI-DSS LV1, Tier III)

Datu centri un mākoņpakalpojumi

250+ industrijas tehnoloģiju eksperti

Informācijas tehnoloģiju konsultācijas

24/7 SOC (650 Milj Logi/dienā), Drošības auditi, u.c.

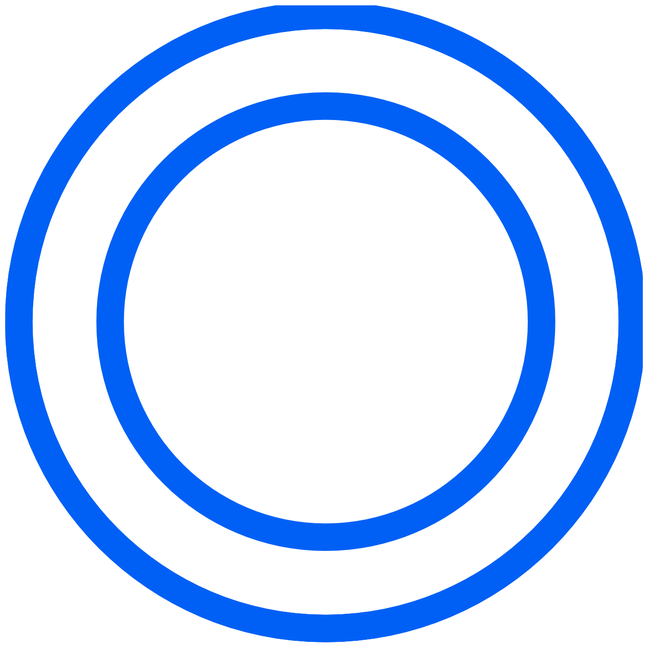
IT drošības pakalpojumi

Kas jauns - **KIBERDROŠĪBĀ**

Tradicionālie **KIBERDROŠĪBAS RISINĀJUMI** vairs nedarbojas efektīvi

Kas jauns - PERIMETRS

Kāds ir mūsu infrastruktūras **PERIMETRS**? Kur tas ir?



Kas jauns – DATU PERIMETRS

Kuri ir mūsu **DATI**? Kādi tie ir?

Projektu **Dati**

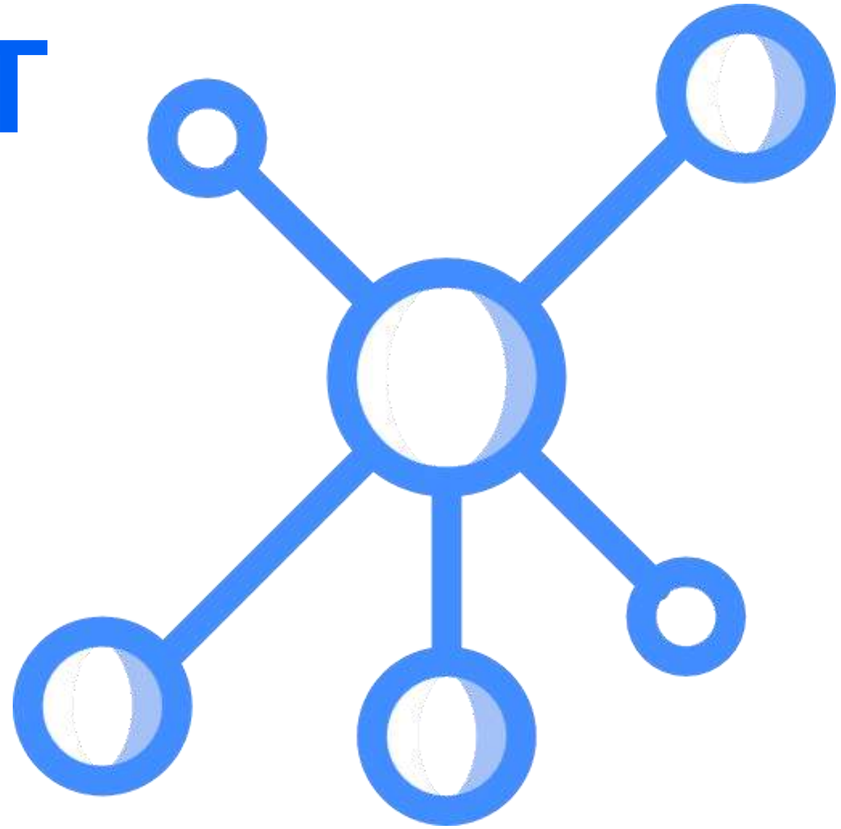
Personas **Dati**

Biznesas **Dati**

Finanšu **Dati**

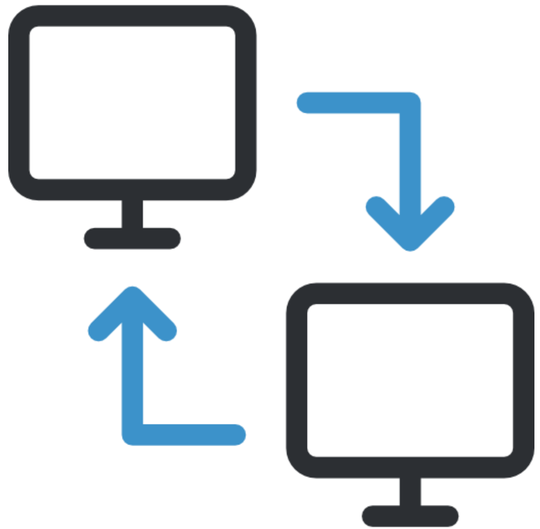
Kas jauns – **SAVIENOTĀS IEKĀRTAS**

Internetam pieslēgto iekārtu skaits **PIEAUG**. Kas vēl tikai būs ar 5G un **IoT**



Kas jauns – IEVAINOJAMI PARTNERI

Cik **KIBERDROŠI** ir mūsu sadarbības partneri? Kas ir ķēdes vājais posms **ŠODIEN?**



Atziņas no IT Drošības Pārbaudēm 2018-2020

Biežāk identificētās IT drošības nepilnības valsts un pašvaldību iestādēs (1/3)

- **IT drošības organizācija/ IT drošības pārvaldnieks (16/30)**
  - Pienākumu atdalīšana
  - Netiek pildīti darba pienākumi
  - Formāla nozīmēšana – IT administrators, teh. resursu turētājs, IT vadītājs, Juridiskās nodaļas vadītājs
- **Netiek apzināti visi IT resursi un netiek veikta sistēmu klasifikācija (29/30)**
- Netiek ierobežota fiziskā piekļuve (9/30)
- **Netiek uzstādīti atjauninājumi (Software/Firmware) (29/30)**
- **Netiek atspējoti nevajadzīgi servisi (18/30)**

Biežāk identificētās IT drošības nepilnības valsts un pašvaldību iestādēs (2/3)

- **Tiek izmantota nedroša attālinātā piekļuve resursiem (29/30)**
- **Netiek izmantots vai nepareizi konfigurēts Ugunsmūris (14/30)**
- **Netiek veikta korekta rezerves kopiju veidošana, glabāšana un atjaunošana (28/30)**
- **Nepilnības lietotāju kontu pārvaldībā (30/30):**
  - Centralizācijas trūkums
  - Paroļu politikas pārkāpumi
  - Paroļu saglabāšana interneta pārlūkprogrammās
  - Koplietošanas kontu izmantošana
  - Pārmērīgu pieejas tiesību piešķiršana

Biežāk identificētās IT drošības nepilnības valsts un pašvaldību iestādēs (3/3)

- **Auditācijas pieraksti (30/30):**
  - Netiek veidoti
  - Netiek uzglabāti ārpus avota noteikto laika periodu
  - Netiek sinhronizēts laiks (NTP)
  - Netiek veikta analīze un reakcija uz incidentiem
- **Vēlreiz neaizmistam par IoT iekārtām!**

MK 442 prasības bieži netiek ievērotas, jo trūkst kontroles mehānisma

Kas vieno šos Latvijas uzņēmumus?

Pašvaldības Restorāni Valsts

Iestādes **Studentu Viesnīcas**

Tehnikumi Top500 Uzņēmumi

IT Pakalpojumu Uzņēmumi

NOTĀRI

Sveiki!

Paldies, ka savā ikdienā izmanto Tet sniegtos pakalpojumus.
Lai saņemtie pakalpojumi vienmēr būtu kvalitatīvi, Tet uztur un seko līdzi tīkla infrastruktūras drošībai, kā arī sadarbojas ar IT drošības incidentu novēršanas institūciju - CERT.LV. Tiklīdz ir konstatēti kādi pārkāpumi vai incidenti, piemēram, datorvīrusa izplatīšanās, lietotājs tiek informēts. Plašāk par drošības prasībām var izlasīt Informācijas tehnoloģiju drošības likumā.

Esam saņēmuši informāciju no CERT.LV, ka Tava lietotā ierīce, iespējams, ir inficēta vai pakļauta ievainojamībai.

Vairāk par infekciju vai ievainojamību var uzzināt šeit:
http://www.esidross.lv/cert-lv-bridinajums/?hash/b965ee90669ee1824ec7567a19828642

Statiskas IP adreses, platjoslas pieslēgumu servisa numuri, kuri izplata infekciju un pārkāpuma datums:

Attieksme pret IT Drošību

Kiberdrošība ir IT Administratora problēma

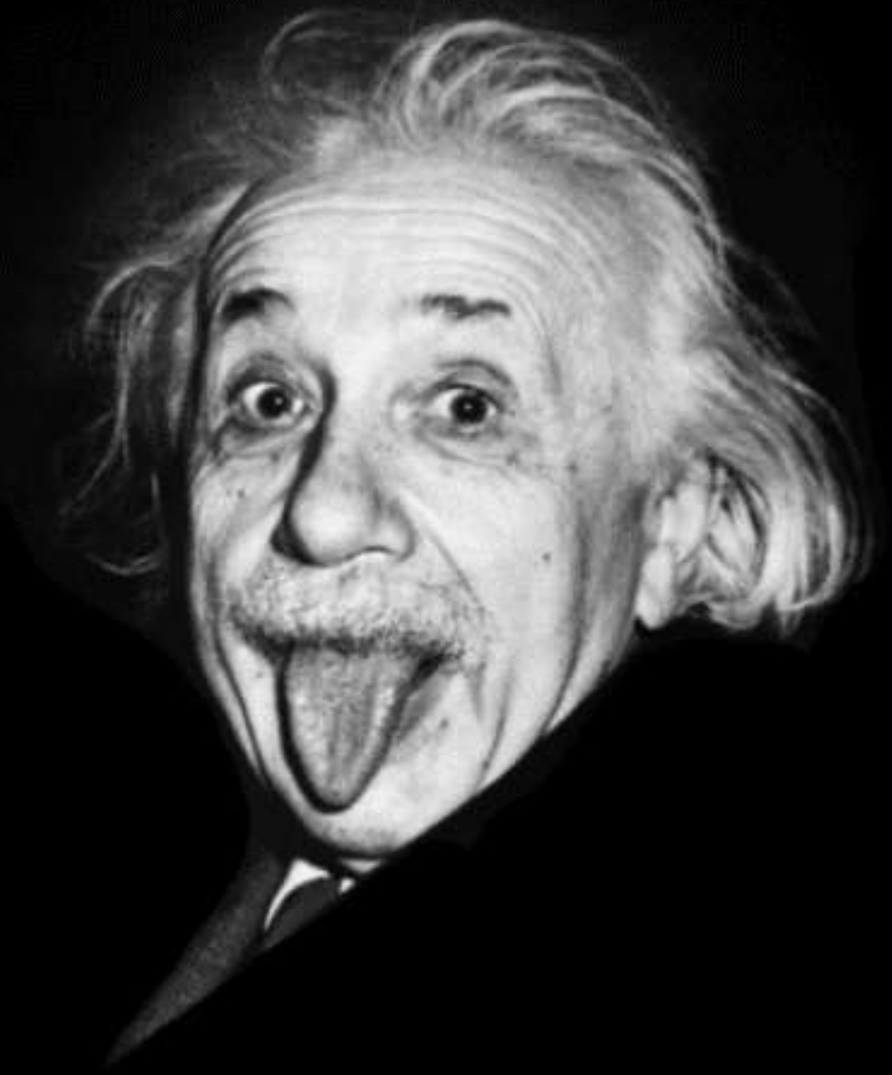
Laba parole pasargās mūs no datu noplūdēm

Uzņēmumi piedzīvo izspiedējvīrusu uzbrukumu ik pēc 40 sekundēm; privātpersonas - ik pēc desmit sekundēm (Apollo.lv)

Mēs uzreiz pamanīsim ka kaut kas nav tā ar IT

"Insanity is doing the same thing over and over again and expecting different results"

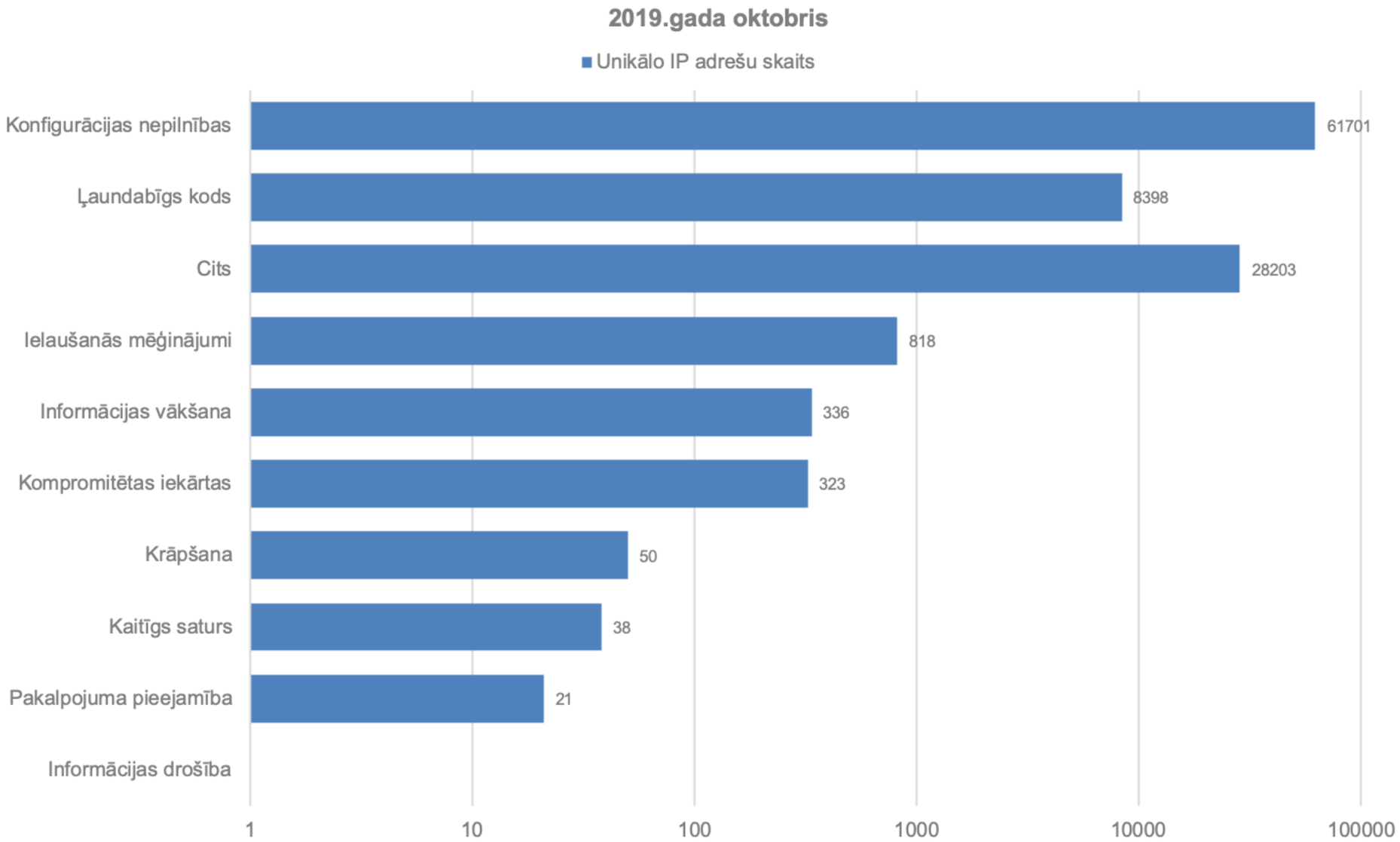
Albert Einstein



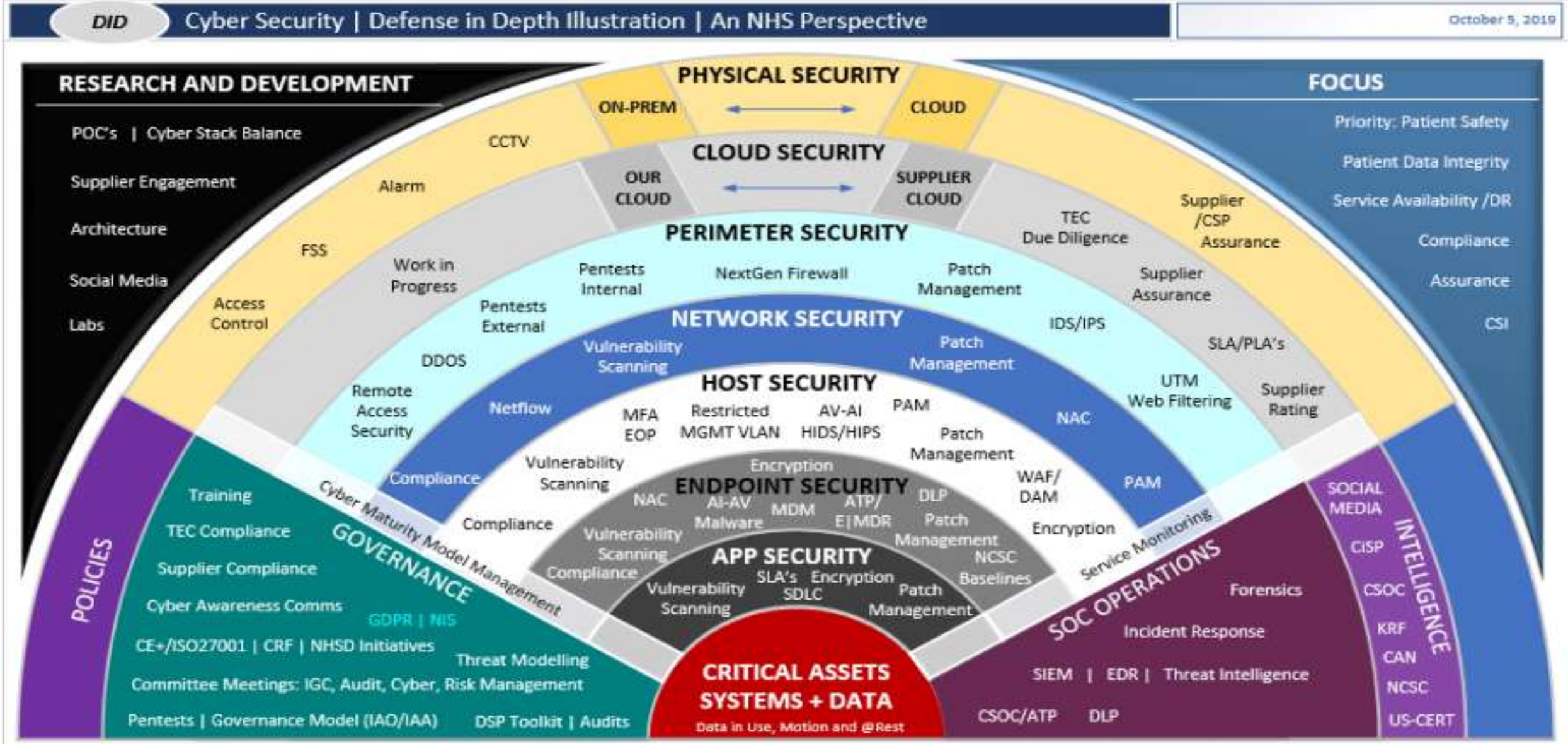
Kāpēc individuāli cīnāmies ar kopējiem KIBER apraudājumiem


Innovācijas
SYS Admin
Tehniskā kompitence
Vīzija un Plāns

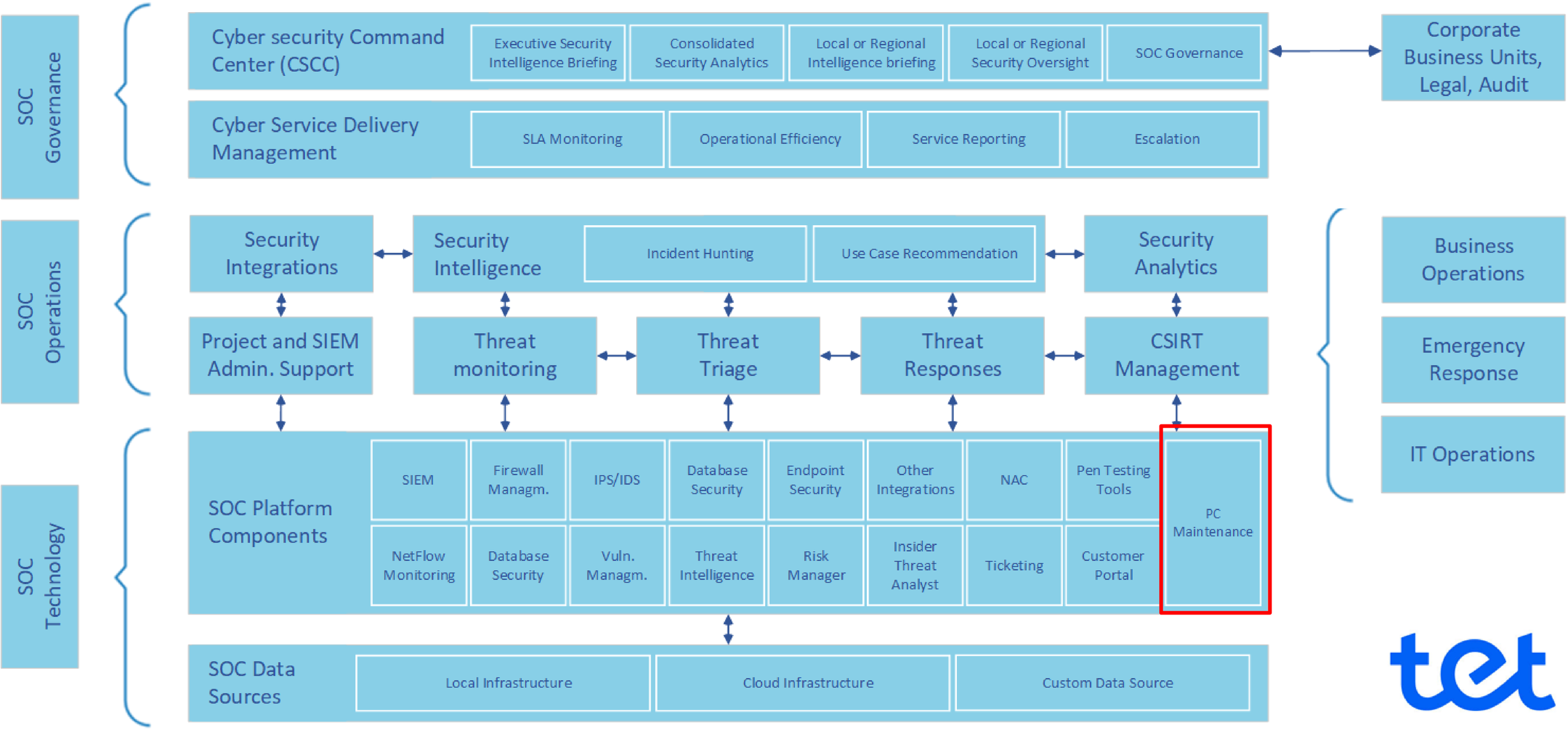
Kas notiek mūsu pagalmā



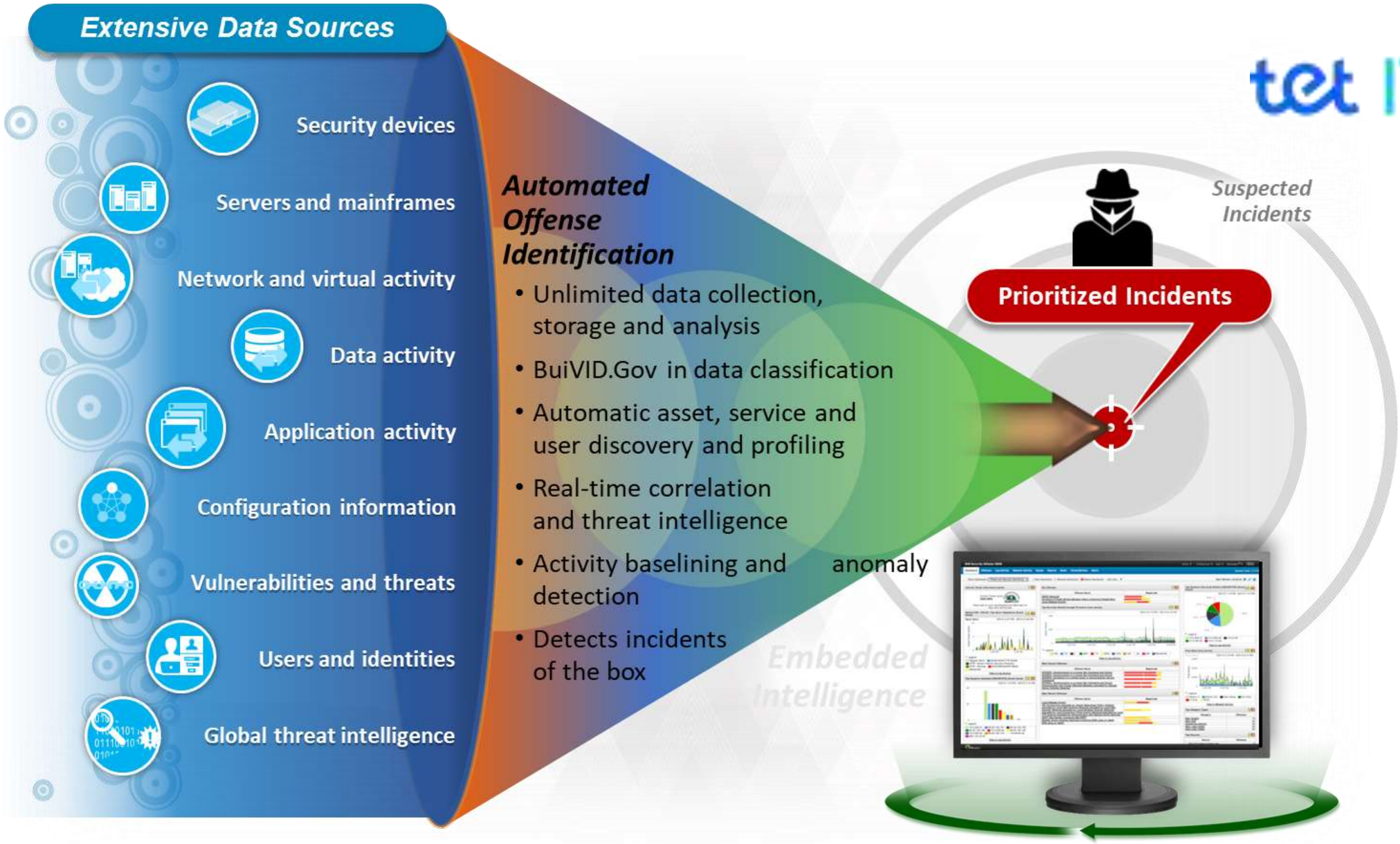
SAVIENOTA/MONITORĒTA/KONTROLĒTA



24/7/365 SOC - Tet



Tet Drošības Vadības Centrs Pašvaldībām



tet IT security

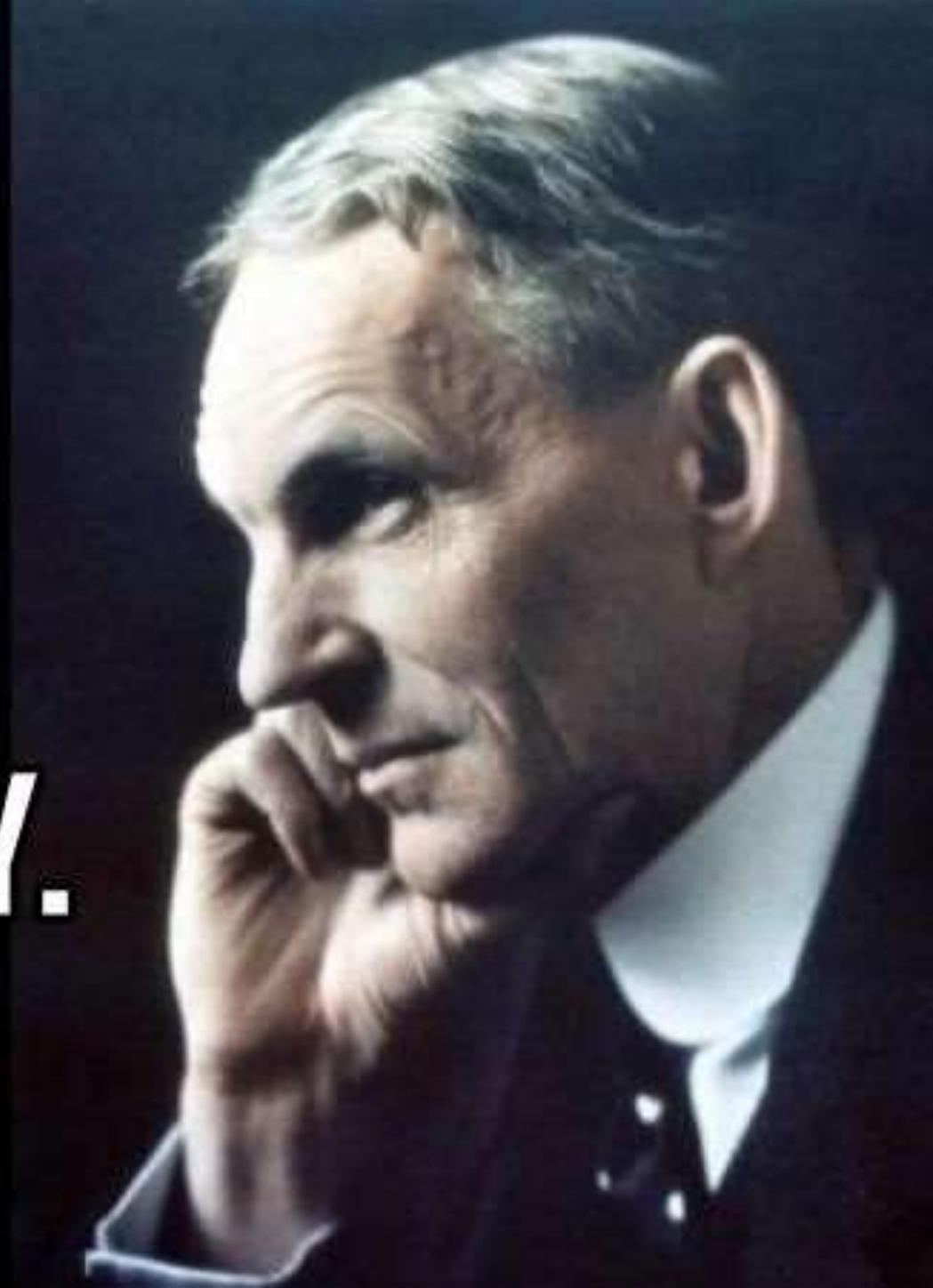
tet

Marketing vs. Reality – TET SOC 24/07/365

We welcome you in
TET SOC Latvia

tet

FAILURE IS THE OPPORTUNITY TO BEGIN AGAIN MORE INTELLIGENTLY.



A security operations platform for todays and tomorrows needs

- Advanced Threat Detection
- Insider Threat
- Securing the Cloud
- Critical Data Protection
- Risk and Vuln Management
- Incident Response
- Compliance

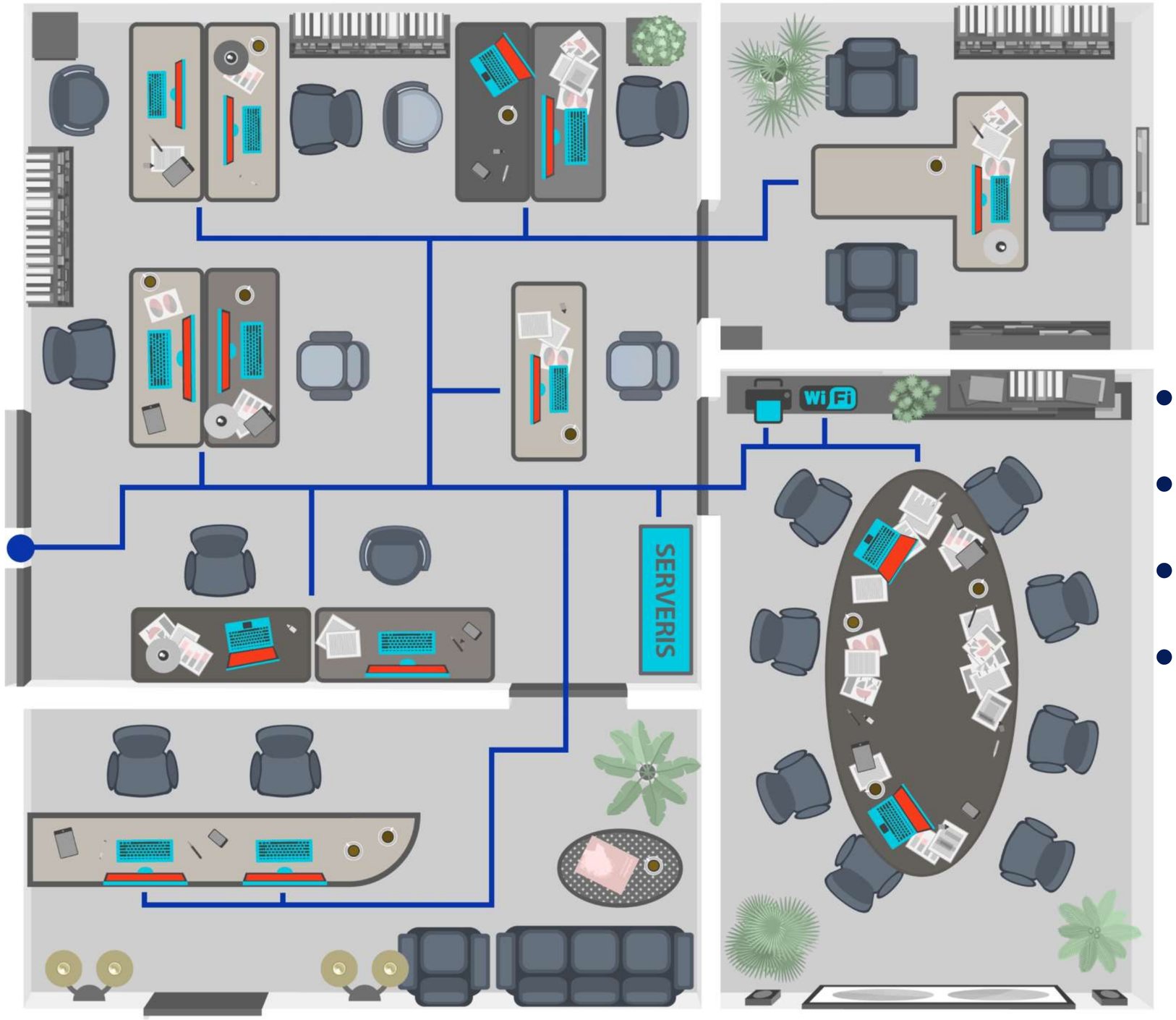
Fast to deploy, easy to manage, and focused on your success

Tet kiberdrošības pakalpojumi

- 24/7 Drošības Vadības Centrs kā pakalpojums
- DDoS novēršanas pakalpojums
- IT ievainojamību Pārvaldības pakalpojums
- Kiberdrošības Analītiķu pakalpojums
- GDPR pakalpojumi
- Datu Aizsardzības un Pārvaldības pakalpojums
- Gala lekārtu Drošības pakalpojums
- IT auditi (ISO, GDPR, PCI…)
- Kiberdrošības Eksperts kā pakalpojums

Datortehnikas apkalpošanas pakalpojumi no IT Drošības puses

Data Experts



Data Experts apkalpo

- Tehnika un iekārtas
- Programmatūra
- Datortīkls
- Pakalpojumi biznesam

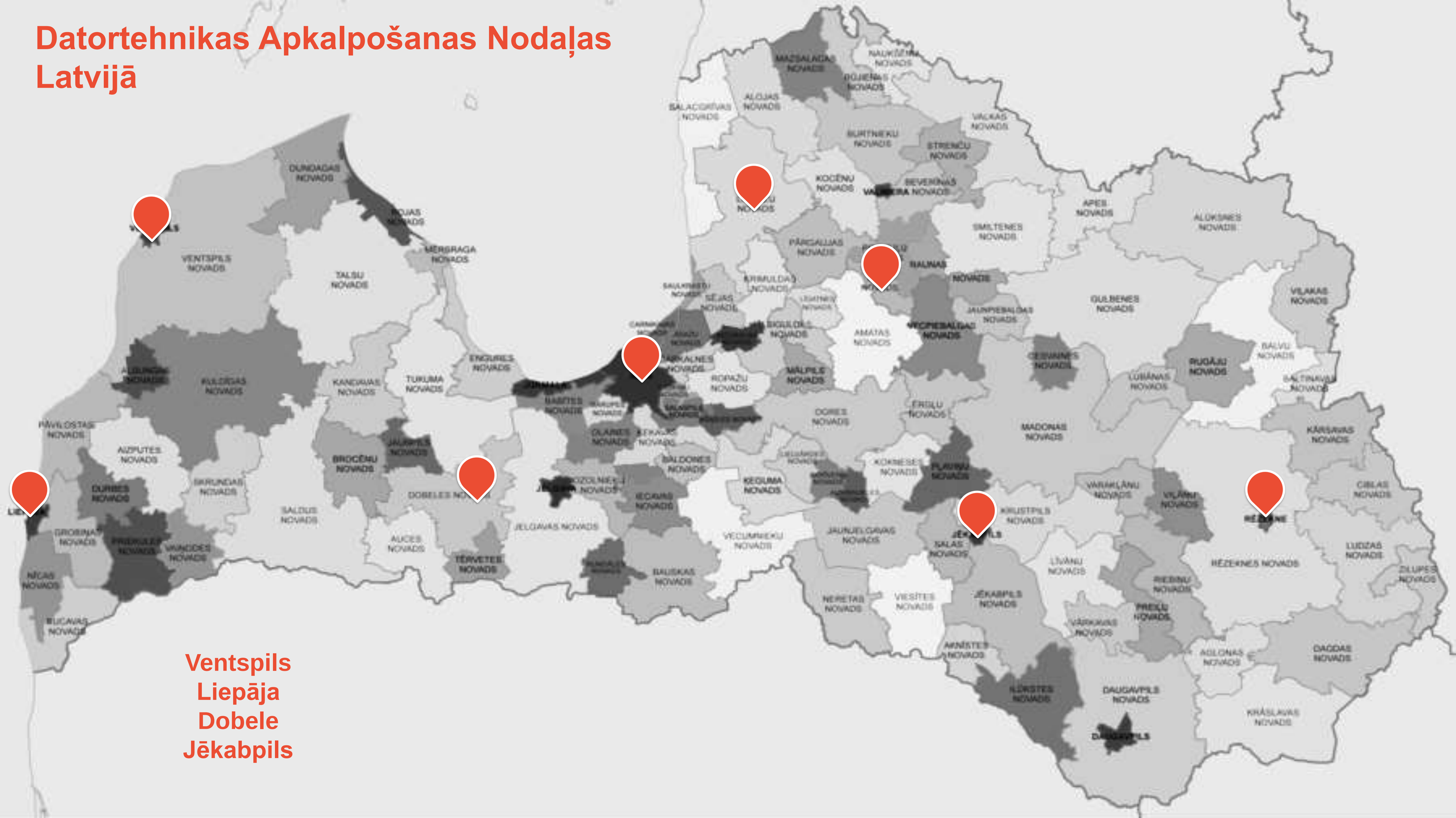
Problēmu risinām jau no pirmā kontakta

Steidzamies palīdzēt:

Gan klātienē

Gan attālināti

Datortehnikas Apkalpošanas Nodaļas Latvijā



Ventspils
Liepāja
Dobele
Jēkabpils

Sadarbības partneri

LATVIJAS VALSTS MEŽI

Coca-Cola

VSAA

SEB

PAŠVALDĪBAS POLICIJA

Uzņēmuma ieguvumi

- Pastāvīga, tūlītēja palīdzība
- Juridiska atbildība
- Finanšu ietaupījumi
- Kvalificēti speciālisti
- Uzskaites sistēma
- Atviegloti grāmatvedības un HR procesi
- IT struktūras uzticamība
- Vienkāršotas iespējas ziņojumiem
- Stabils partneris ar pieredzi

- Klienta piemērs nr.1:
  - Veicot primāro auditu tika konstatēts, ka klientam, katrs darbinieks ir ar administratora tiesībām uz sava datora
  - Ejot prom no darba darbinieks nopludina/izdzēš svarīgu kompānijas informāciju

  - Slēdzot līgumu par ārpakalpojumu –
    - Pirmā mūsu rekomendācija, visiem tika noņemtas administratora tiesības, atstājot tās tikai ierobežotai personu grupai, kas tika saskaņots ar vadību.
    - Pārkonfigurēti e-pasti, lai veidotos back-up,
    - Failu rediģēšanas iespējas konkrētos gadījumos tika noņemtas vai ierobežotas

- Klienta piemērs nr.2:
  - Klientam ar aptuveni 100 lokācijām nebija izveidota vienota aktīvā direktorija, bet bija iespēja piekļūt pie kopējās datu bāzes failiem, kas palielināja risku uz datu nopludināšanu. Klienta darbinieku rīcībā sensitīvie dati.

  - Slēdzot līgumu par ārpakalpojumu:
    - Palīdzējām izveidot vienotu aktīvo direktoriju
    - Ieviesām datu šifrēšanu
    - Izveidojām limitētai personu grupai administratīvās tiesības
    - Palīdzējām veikt patchošanu, lai visiem datoriem būtu vienādas funkcijas

- Klienta piemērs nr.3:
  - Klientam veicot iekšējo analīzi tika konstatēts, ka liels skaits vīrusu tiek saņemti datora tieši caur usb flash drive ierīcēm, kā arī nav pārāk sarežģīti nozagt datus, ja pats dzelzis ir ticis nozaudēts/nozagts.

- Slēdzot līgumu par ārpakalpojumu:
  - Tika veikta Bios paroļu uzstādīšana un Bitlocker datu šifrēšanas nodrošināšana, kas ir viens no efektīvākajiem veidiem, kā samazināt riskus uz datu pazaudēšanu
  - Tika atslēgta chrome paroļu saglabāšana/sinhronizēšanas
  - Flash drive atslēgšana izņemot konkrētos gadījumos

Matīss Mazurenko

Datortehnikas apkalpošanas pakalpojumu vadītājs

M: +371 22 020 817

E: Matiss.Mazurenko@tet.lv

A: Dzirnavu 105, Rīga, LV-1011

Data Expert

Paldies

Thank you

Спаси́бо

Дякуємо