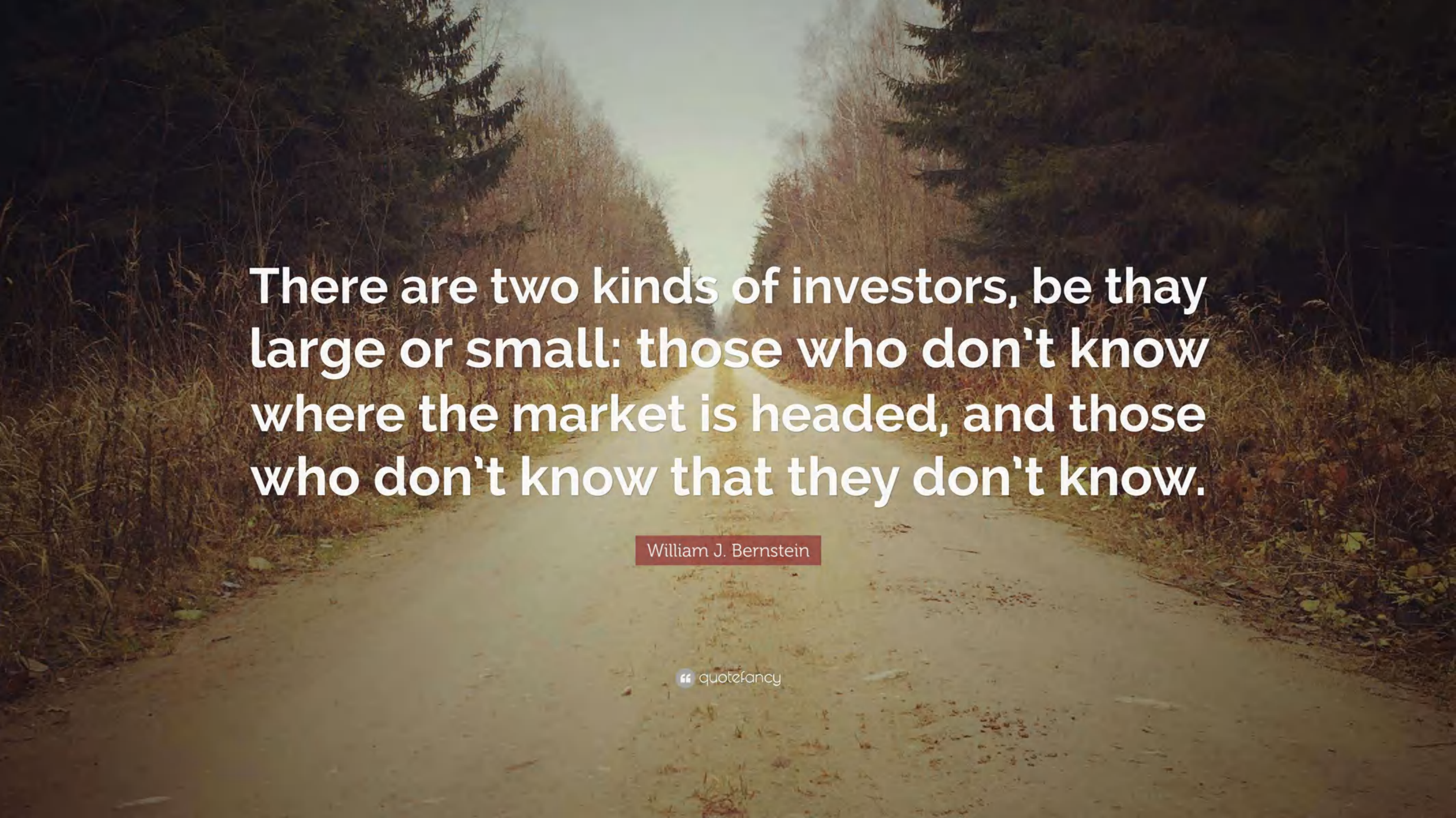
Investē kiberdrošībā, nevis kibernoziedzībā

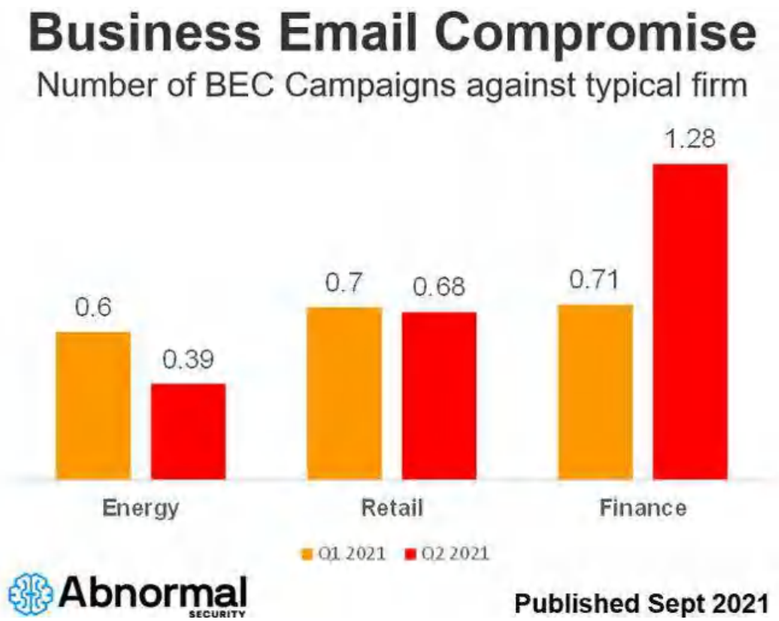
Kāpēc investēt kiberdrošībā ir izdevīgāk?

Artūrs Filatovs
Kiberdrošības pakalpojumu vadītājs

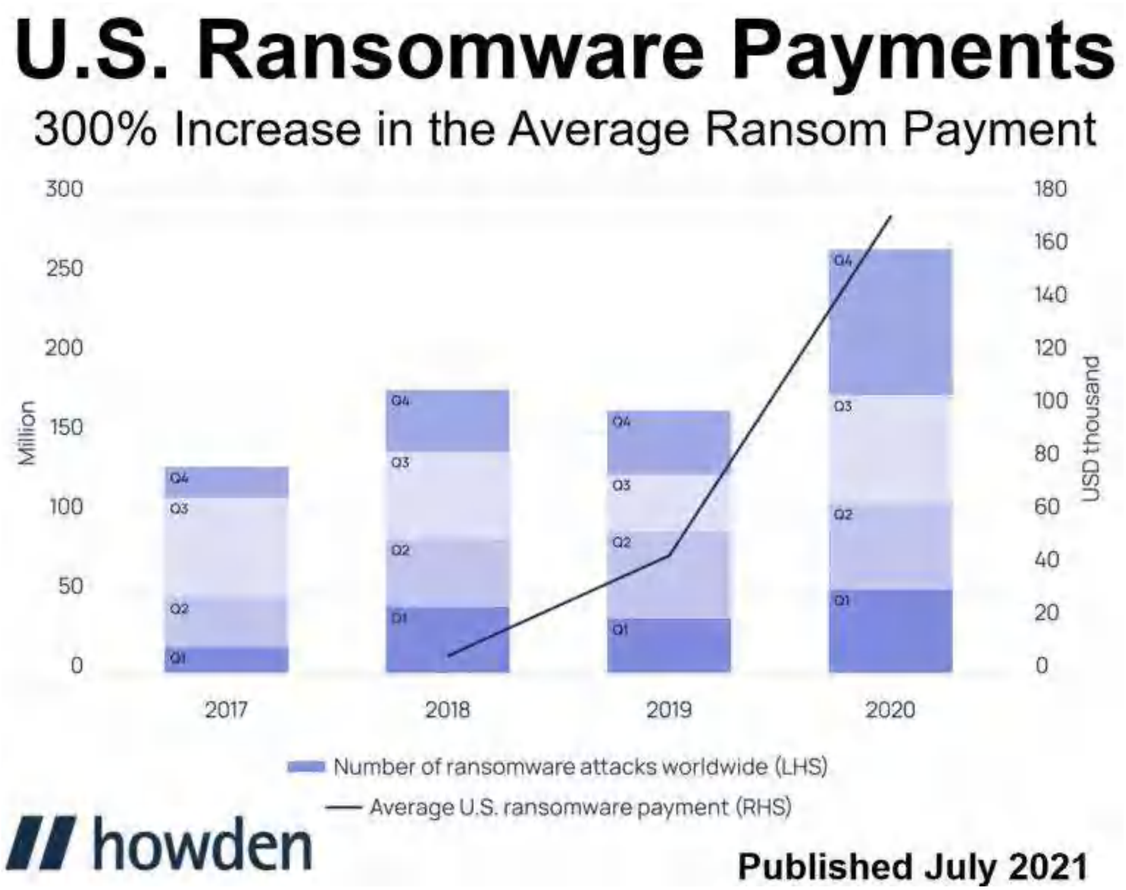

There are two kinds of investors, be thay large or small: those who don't know where the market is headed, and those who don't know that they don't know.
William J. Bernstein
quotefancy

Latvijas kibernoziedznieku investori

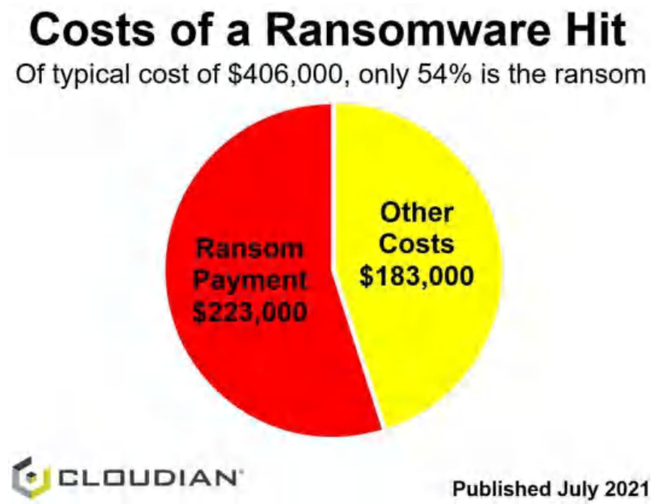
- 31. augustā, VP. Liepājas iecirknis saņēma iesniegumu no kāda uzņēmuma, kurā konstatēts, ka notikusi krāpšana un kopumā radīti zaudējumi 180 000 eiro apmērā.
- 1. septembrī, VP. Valkas iecirknis saņēma iesniegumu no kāda uzņēmuma, kurš šī gada 23.martā saņēma rēķinu no kādas firmas Zviedrijā par ekskavatora iegādi 11 500 EUR un veica samaksu
- Šogad pie Tet vērsās Latvijas transporta kompānija, kuras datus kibernoziedznieki jau bija nošifrējuši, un viņiem nācās samaksāt 60 tūkstošus eiro



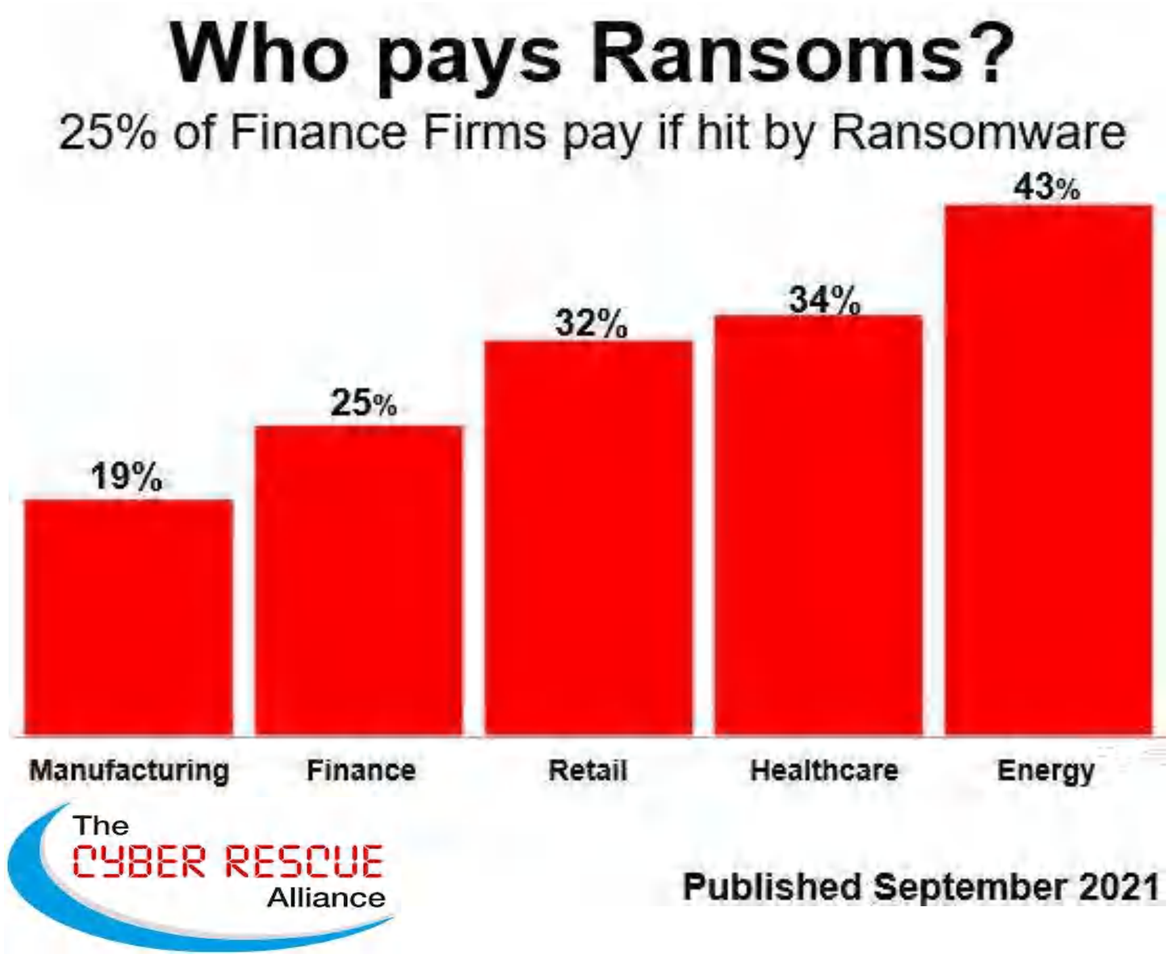
Cik mēs investējam kibernoziedzībā?

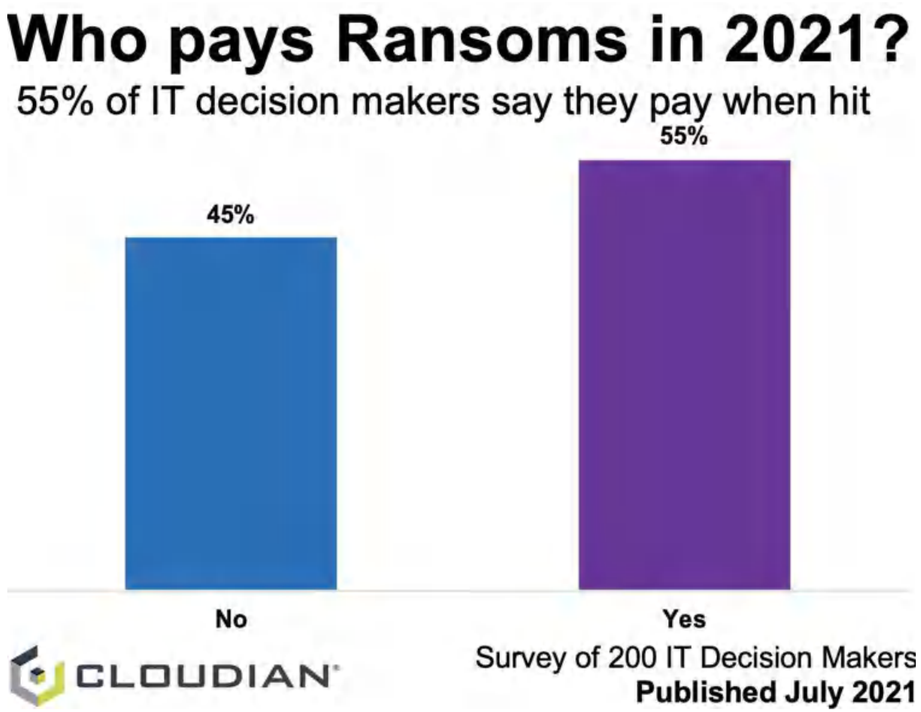


Neilgi pēc uzbrukuma Colonial nolēma samaksāt izpirkuma maksu 75 bitkoiniem, kas tobrīd tika novērtēti aptuveni 4,4 miljonu $



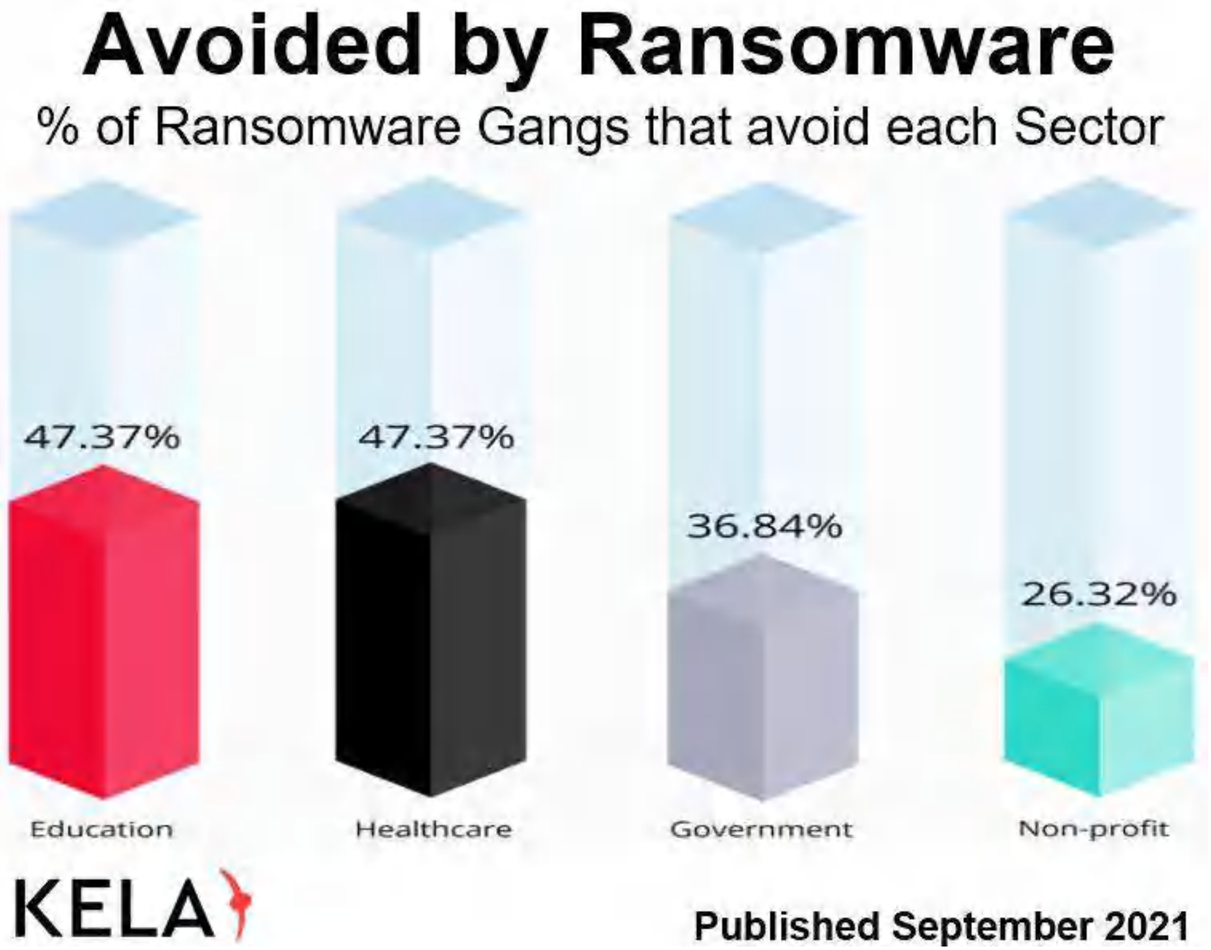
Kuri ir kibernoziedznieku galvenie investori?





Atgūšanas izmaksas un dīkstāves pēc izpirkuma programmatūras uzbrukuma, kā arī kaitējums reputācijai var būt 10 līdz 15 reizes vairāk nekā izpirkuma maksa.

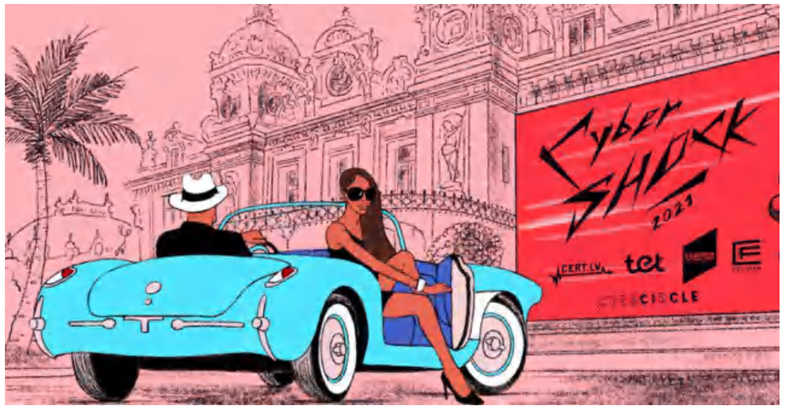
Kādi investori ir kibernoziedznieki?



Kibernoziedznieki izvēlas investēt savus resursus ar mazākiem riskiem un finansiāli izdevīgāk

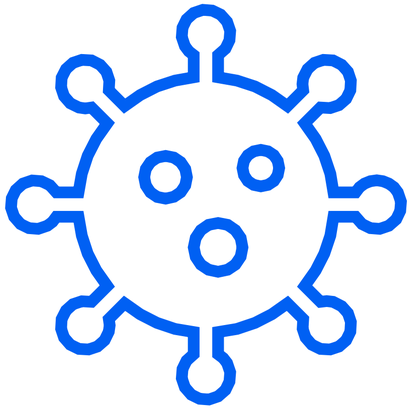
Cik viegli ir nopirkt datus par Latviju?

Tet Dark Web Threat Intelligence serviss

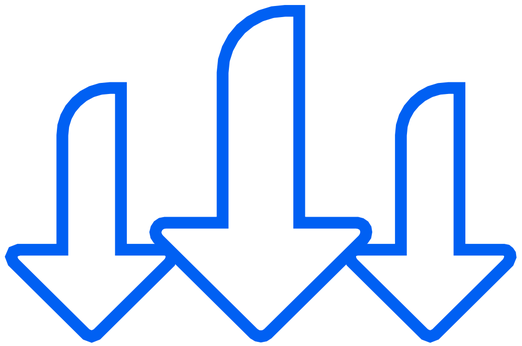


Kibernoziedzniekiem nav atvaļinājumu

Par 50% vairāk apturētu e-pastu ar vīrusiem **72 000**



Jauna tipa vīrusu izplatība ar **.edoc**



Apturēti **2 050 Ddos** uzbrukumi. Agresīvāki, ilgāki, sarežģītāki

Kas vieno šos Latvijas uzņēmumus?

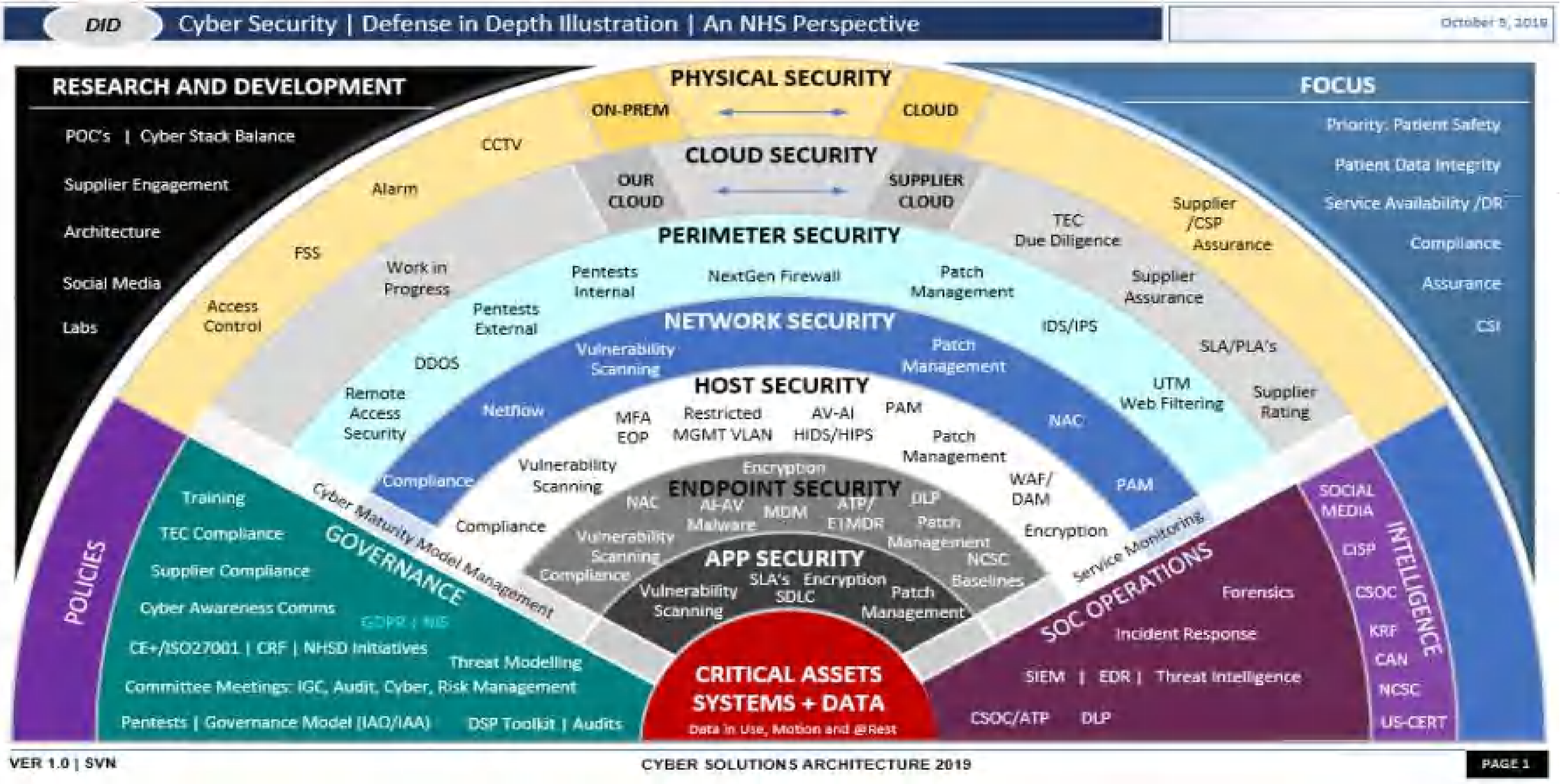
Pašvaldības Restorāni Valsts
Iestādes Studentu Viesnīcas
Tehnikumi Top500 Uzņēmumi

IT Pakalpojumu Uzņēmumi
NOTĀRI

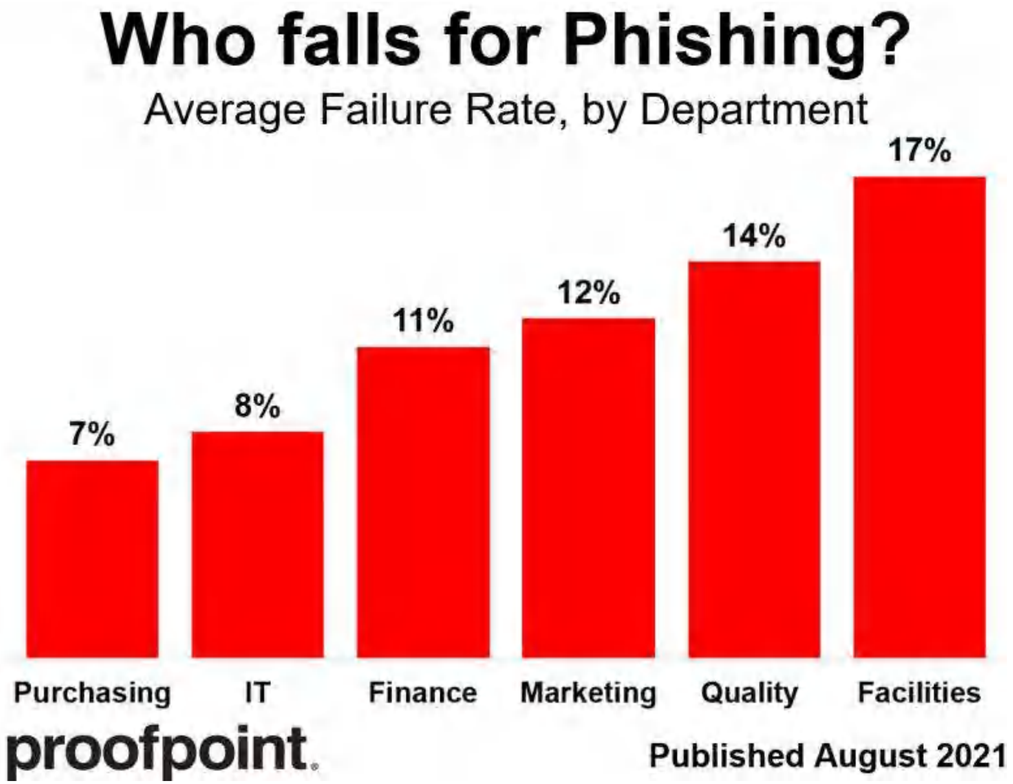
Mēs uzreiz pamanīsim, ka kaut kas nav tā ar IT

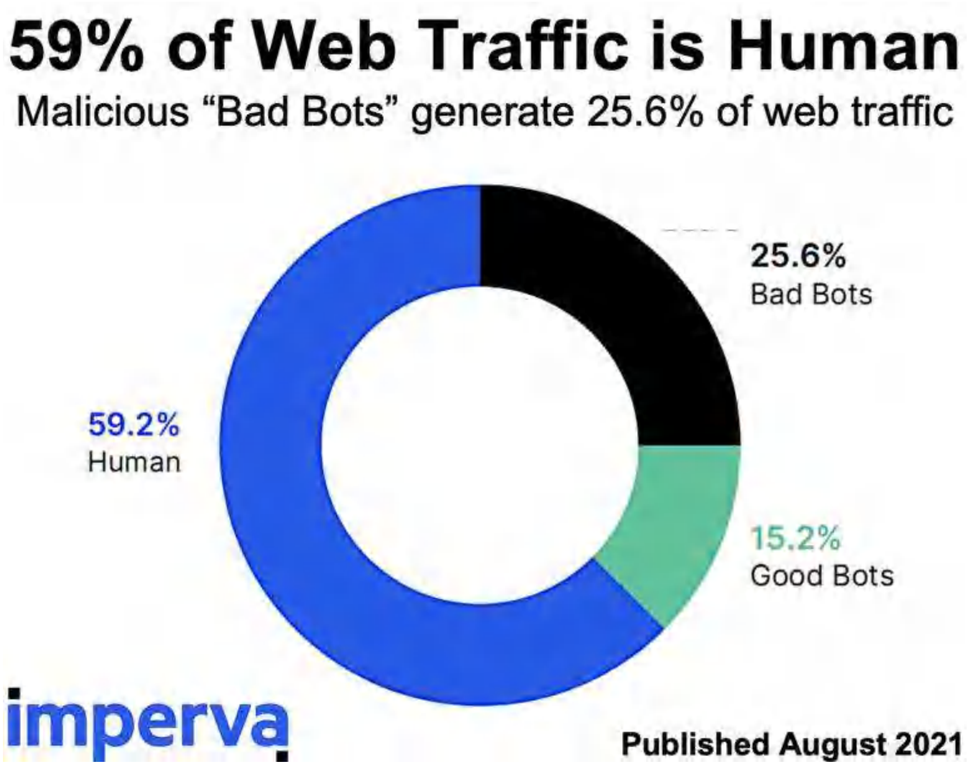
Kiberdrošība ir IT Administratora problēma

Kāpēc tad mēs nepamanām uzbrukumus?

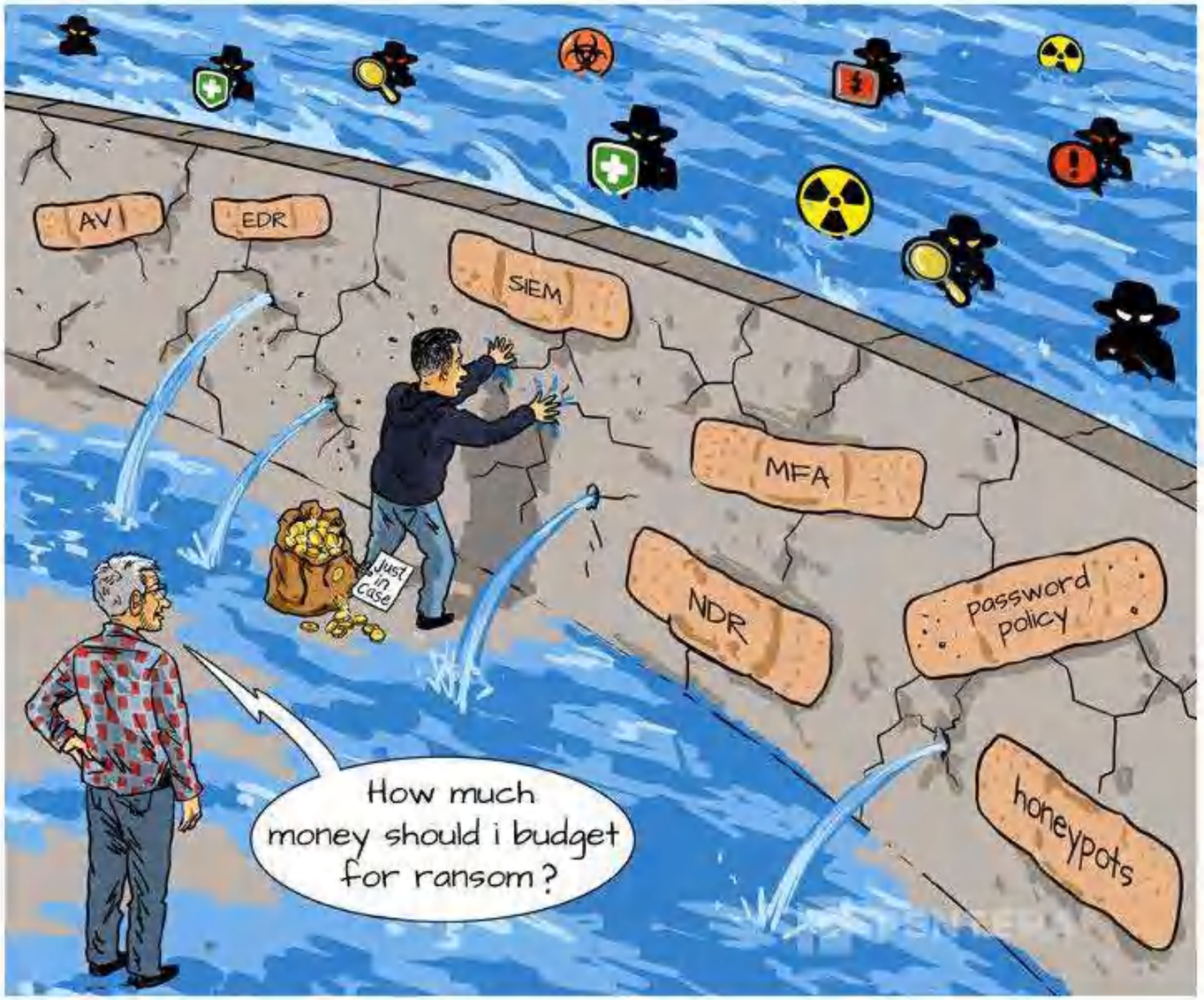


Kāpēc tad mēs nepamanām šo?





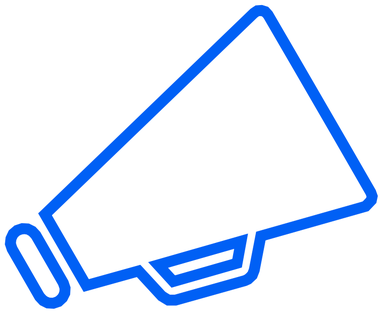
Cik kvalitatīvas ir mūsu sienas?



Mēs arī strādājam 24/7/365

SOC - Monitorings

Pilna cikla kiberdrošības pakalpojumi



Informējam privāto/publisko sektoru sadarbībā ar CERT.LV

~ 240 milj. mēnesī auditācijas pierakstu par notiekošo mūsu un tīklā mūsu tīklā un pie mūsu klientiem

Drošības izmeklēšanas darba plūsma:

Incidenta atklāšana

Drošības incidenta atklāšana var notikt dažādos veidos:

- Pārkāpums tiek atklāts manuāli;
- Atklātas aizdomīgas darbības vai notikums;
- Kāda no drošības uzraudzības sistēmām atklāj drošības incidentu un paziņo par to;
- Drošības analītiķis atklāj aizdomīgas darbības vai incidentu.

Sākotnēja izmeklešana

Sākotnēji zināmās informācijas ievākšana un apkopošana:

- Cēlonis;
- Tīkla informācija;
- Riska līmenis;
- Iesaistītie lietotāji;
- Noskaidrot, vai nepieciešama padziļināta izmeklēšana;
- Klienta informēšana par drošības incidentu.

Kategorizē-šana

Tiek noteikts:

- Konkrēts incidenta risks;
- Notikušā incidenta ietekme un sekas;
- Tehniskā resursa stāvoklis.

Izmeklēšana

Visas nepieciešamās informācijas ievākšana, apkopošana un padziļināta izpēta, lai noskaidrotu:

- Galveno incidenta iemeslu;
- Iespējamās darbības incidenta seku novēršanai;
- Preventīvās darbības.

Risinājums

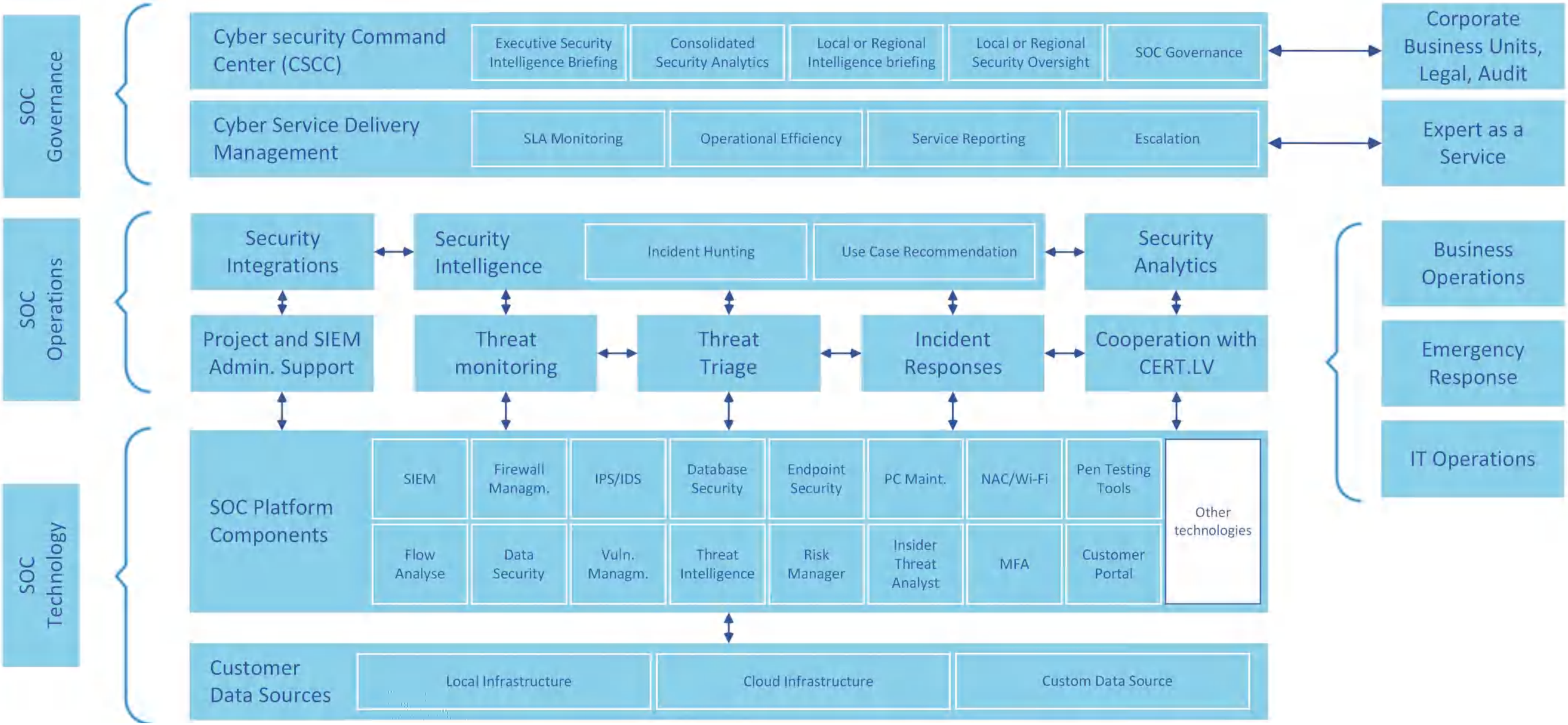
- Pielāgota un individuāla risinājuma sniegšana, kas piemērots konkrētajam incidentam;
- Konsultāciju sniegšana saistībā ar incidenta atrisināšanas aktivitātēm;
- Risinājuma soļu veikšanas ieviešana un uzraudzība.

Secinājumi

Līdz ar incidenta ietekmes vai seku novēršanu:

- Tiek slēgta incidentā izmeklēšana
- tiek apkopota visu veikto darbību informācija un iekļauta vienotā vai īpaši pielāgotā nodevumā;

24/7/365 SOC - Tet



Daži no kiberdrošības pakalpojumiem

- **SIEM** svarīga datu drošības ekosistēmas daļa: tas apkopo datus no vairākām sistēmām un analizē tos, lai noķertu neparastu uzvedību vai iespējamus kiberuzbrukumus;
- **Network monitoring** - palīdz administratoriem un drošības speciālistiem atrisināt tīkla veiktspējas problēmas, noteikt kļūdainas funkcijas un aizsargāt no kiberdraudiem;
- **Firewall** - ir drošības sistēma, kas ievieto speciāli ieprogrammētu datoru starp organizācijas vietējo datortīklu un internetu. Tas aizsargā uzņēmumu no interneta lietotāju nesankcionētas piekļuves;
- **Database/ data security** - aizsargājiet kritiskos uzņēmuma datus un kontrolējiet piekļuvi datu uzglabāšanas sistēmās un datu bāzēs;
- **IPS / IDS / DDos** - analizē uzņēmuma IT tīklu, lai identificētu kiberdraudus un apturētu kiberuzbrukumu, tādējādi pasargājot uzņēmumu;
- **Vulnerability management** - modulis programmatūras ievainojamību identificēšanai, klasificēšanai, prioritāšu noteikšanai, novēršanai un novēršanai;
- **Threat intelligence** – iespējamo kiberdraudu informācijas ievākšana un apkopošana, kas palīdz pasargāt uzņēmumu no jauniem kiberuzbrukumiem;

Kāpēc pakalpojums nevis produkts?

Izdevīgi (CAPEX un OPEX)
Data experts drošības vadības centra pakalpojums **sākot ar 900 eiro mēnesī**.

Pievienotā vērtība
Iespēja efektīvi izvērtēt un atsekot kiberdrošības un datu procesus un uzlabot tos. Labs palīgs jebkuram IT un drošības vadītājam.

Ērta pārvaldība
Drošības vadības centrs apvieno dažādas IT un IT drošības sistēmu datus, rīkus un informāciju par tām vienā platformā, kas ļauj ērti pārvaldīt uzņēmuma kiberriskus.

Aizsardzība pret kiberuzbrukumiem (proaktīvi)
Kiberdrošības eksperti iesaistās Jūsu IT infrastruktūras aizsardzībā un jaunu politiku izstrādē, lai mazinātu riskus
kiberuzbrukuma laikā vai pirms tā.

Kiberdrošības monitorings
Nepārtraukts kiberdrošības sistēmu monitorings, kas efektīvāk palīdzēs aizsargāties, gan no iekšējiem, gan ārējiem apdraudējumiem.

Pielāgošana
Data Experts drošības vadības centru ir iespējams ērti un automatizēti pielāgot jau esošajām uzņēmuma IT drošības sistēmu komponentēm.

Paldies!

Kontakti

Arturs.Filatovs@tet.lv

27194080