

PASTAIGA PA SOC DŽUNĢIEM

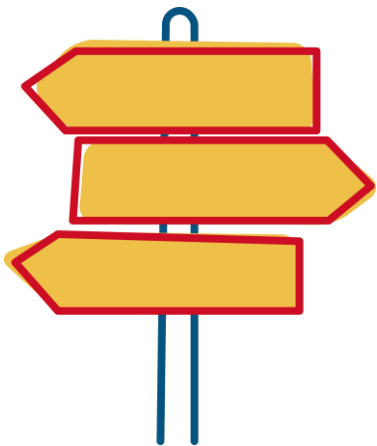
Kā nenomaldīties lēmumu
krustcelēs?

Artūrs Filatovs

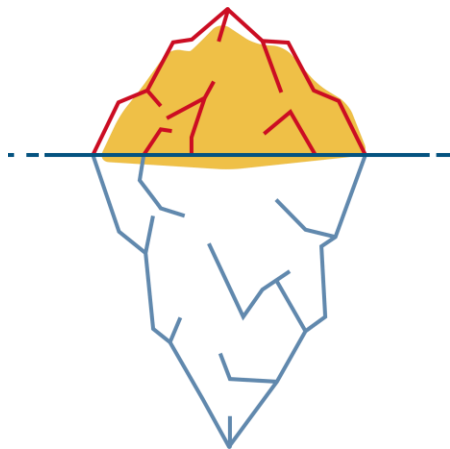
LVRTC / Kiberdrošības biznesa virziena vadītājs
ENISA / LV delegētais Kiberdrošības Eksperts



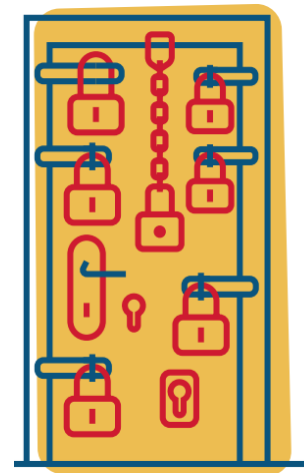
KAS IR KIBERDROŠĪBAS DŽUNGLI?



Dažādi risinājumi
un pieejas



Pieeja kiberhigiēnai ir
virspusēja



Pārāk liela
kiberdrošība ir lemta
neveiksmei!

KURU CEĻU IZVĒLĒTIES?

PAŠBŪVĒTS SOC

SOC KĀ PAKALPOJUMS
(SOCaaS)

OPEN SOURCE SOC

LVRTC SOC PIEREDZĒTAIS

9+
SPECIĀLISTI

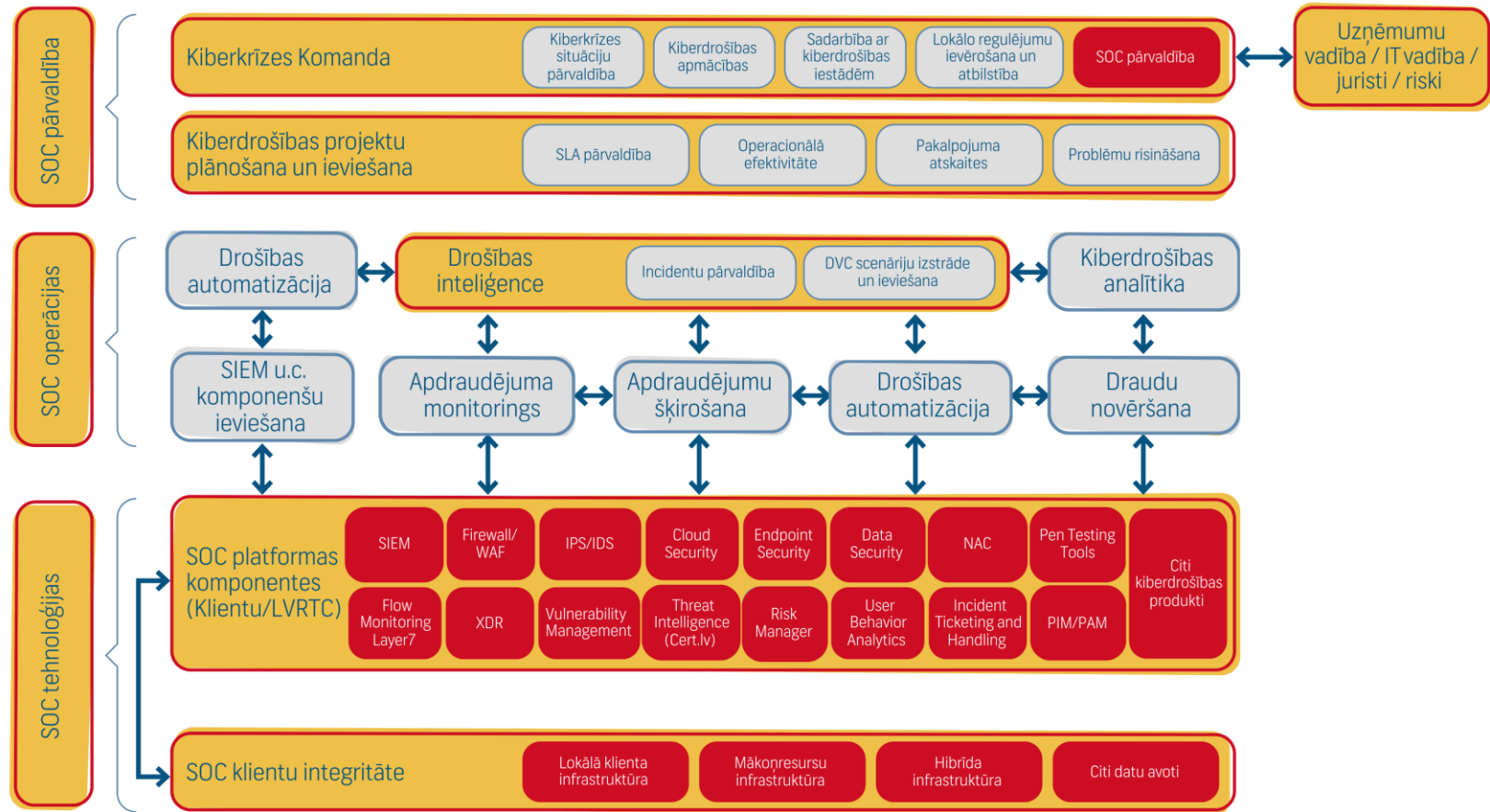
8+
KIBERDROŠĪBAS
PAKALPOJUMI

18 000+
PIKŠĶERĒŠANAS
SIMULĀCIJAS

3 460+
SOC

750K
ATVAIRĪJUMU MĒNESĪ

SOC PAŠBŪVES ARHITEKTŪRA



ATBILSTĪBA UN UZTURĒŠANA

MK397/NKDL, DORA u.c.

SOC kā
pakalpojums
(SOCaaS)

MK397
NKDL

Gatava atbilstība

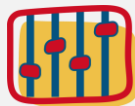


Iekļauta dokumentācija



Uztur pakalpojuma sniedzējs

Pašbūvēts SOC



Jābūvē procesi pašam



Manuāla dokumentācija



Uztur iekšējā komanda

Open-source
SOC



Nav garantijas

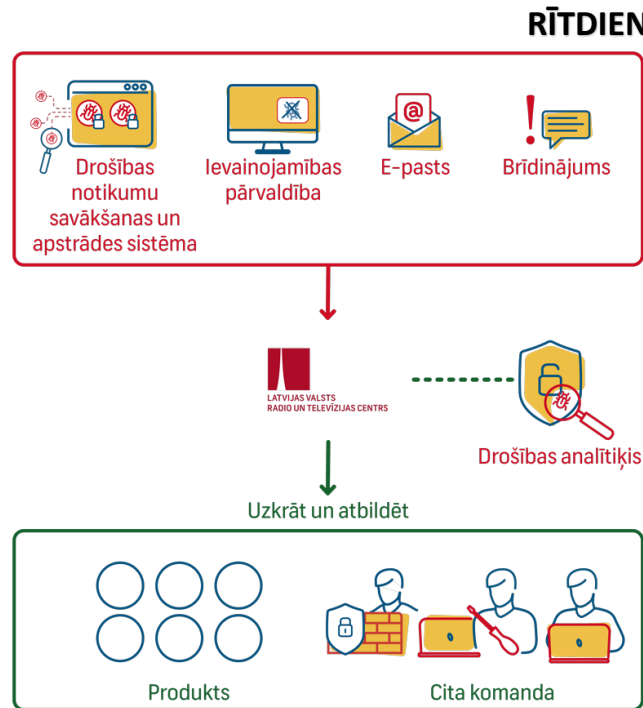
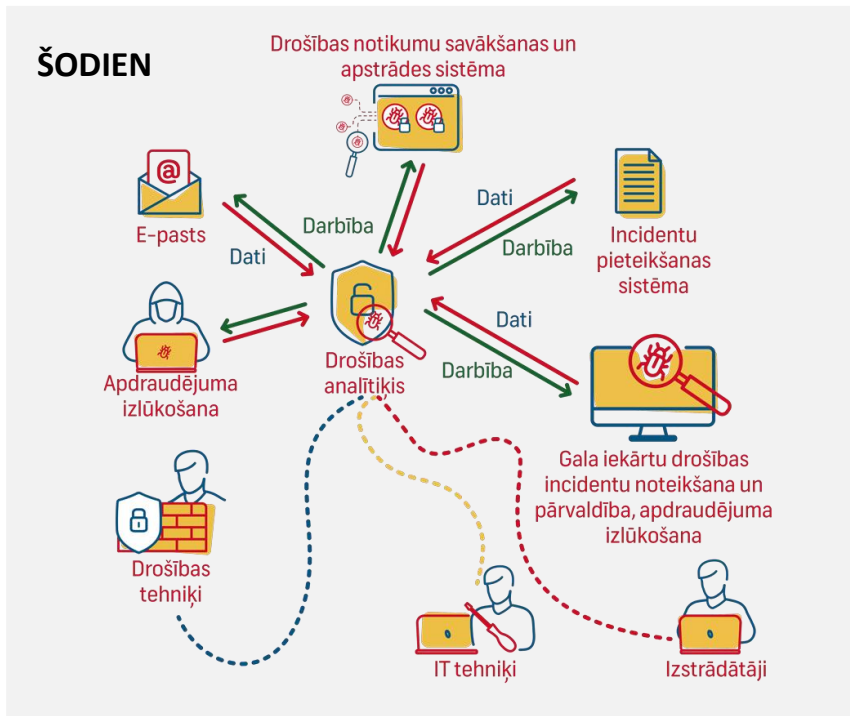


Patērē daudz resursu



Manuāli atjauninājumi

UZLABOTS PROCESS - UZLABOTA DROŠĪBA



INCIDENTU ATKLĀŠANA, REAĢĒŠANA UN ATSKAITE (24/7/30)

SOC kā
pakalpojums
(SOCaaS)



Ātri, automatizēti



SOAR + AI iespējas



Regulāras atskaites

Pašbūvēts SOC



Atkarīgs no komandas



Manuālas atskaites



Integrācija + zināšanas

Open-source
SOC



Pieejami bezmaksas rīki



Jāizstrādā pašiem



Ziņošana jāpielāgo normatīviem

LVRTC SOC DROŠĪBAS IZMEKLĒŠANAS DARBA PLŪSMA:

Incidenta atklāšana

- Manuāli vai identificējot aizdomīgas darbības
- Drošības uzraudzības sistēma paziņo par incidentu
- SOC analītiķis atklāj aizdomīgu aktivitāti
- Var tikt novērsti atbilstoši SOC politikām

Sākotnēja izmeklēšana

- Tiek apkopots:
- Incidenta cēlonis
 - Tīkla informācija
 - Riska līmenis
 - Iesaistītie lietotāji
 - Novērtē, vai nepieciešama padziļināta izmeklēšana
 - Veikta klienta informēšana par incidentu.

Kategorizēšana

- Tiek noteikts:
- Konkrēts incidenta risks
 - Notikušā incidenta ietekme un sekas
 - Tehniskā resursa stāvoklis

Izmeklēšana

- Informācijas padziļināta izpēte, lai noskaidrotu:
- Galveno incidenta iemeslu
 - Iespējamās darbības incidenta seku novēršanai
 - Preventīvās darbības.

Risinājums

- Incidenta novēršana izmantojot SOC tehnoloģijas
- Piedāvāts pielāgots risinājums
- Konsultāciju sniegšana incidenta atrisināšanā
- Risinājuma izpildes uzraudzība

Secinājumi

- Līdz ar incidenta ietekmes vai seku novēršanu:
- Incidenta izmeklēšanas slēgšana
 - Veiktās darbības dokumentētas vienotā vai pielāgotā pārskatā

IZMAKSAS UN MĒROGOJAMĪBA

SOC kā
pakalpojums
(SOCaaS)



Abonēšanas modelis



Nav sākotnējā ieguldījuma



Ātri pielāgojams apjomam

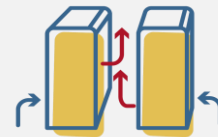
Pašbūvēts SOC



Lieli sākuma ieguldījumi



Nepieciešami cilvēkresursi



Papildu infrastruktūra

Open-source
SOC



Zemas licences
izmaksas

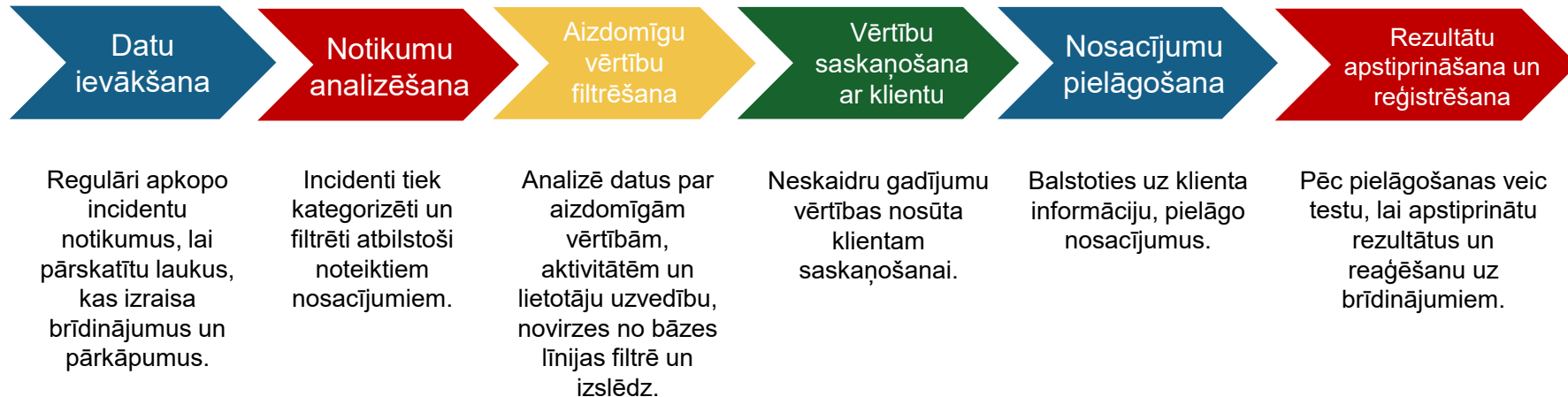


Augstas uzturēšanas
izmaksas



Mērogojamība atkarīga
no resursiem

POLITIKU PIELĀGOŠANAS DARBĪBU PLŪSMA



AUDITS UN EKSPERTĪZE

SOC kā
pakalpojums
(SOCaaS)



Pieejamas SOC ekspertu zināšanas



Gatava audita dokumentācija

Pašbūvēts SOC



Ekspertīze atkarīga no iekšējās komandas



Manuāla audita dokumentācija

Open-source
SOC



Nepieciešamas augsta līmeņa zināšanas



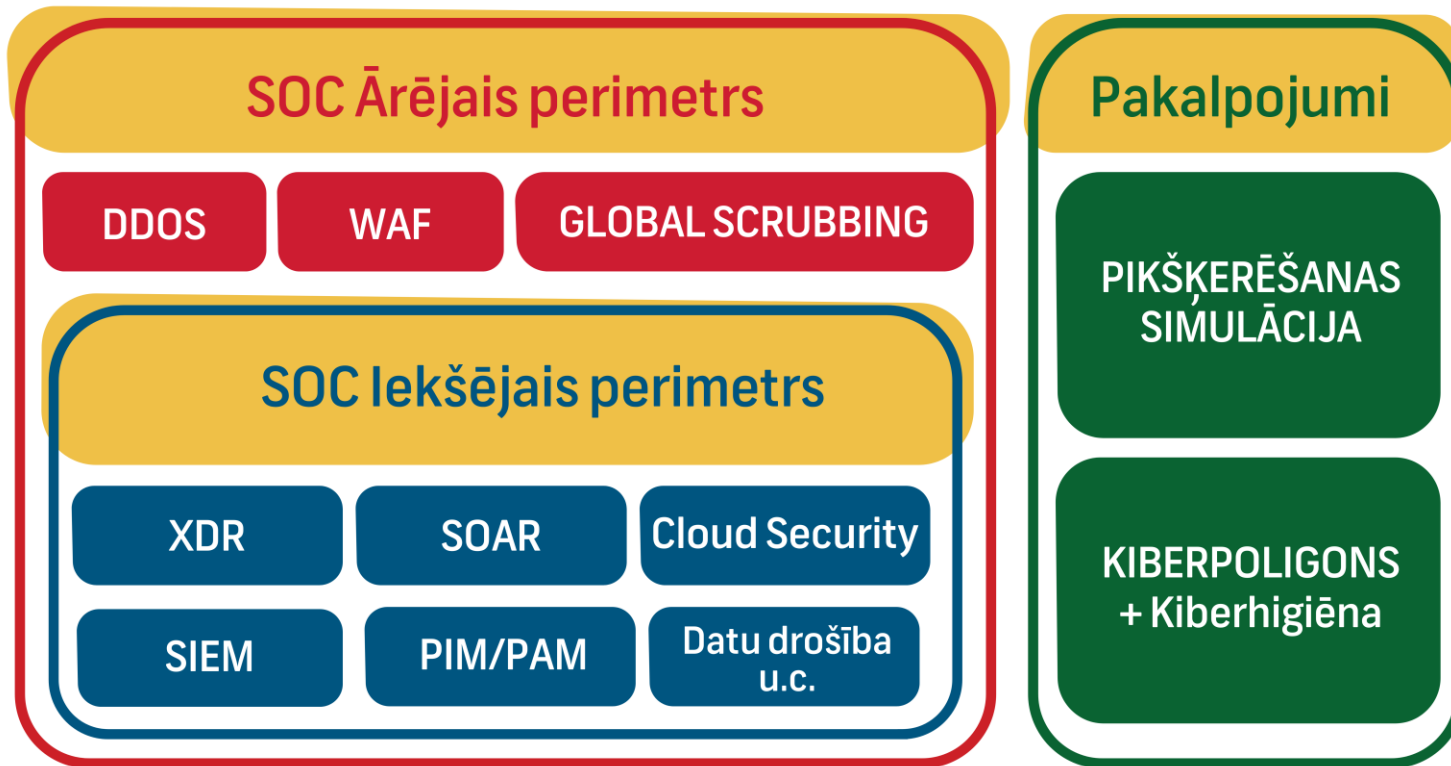
Pieejami žurnāli, audits - manuāli

BEZ SOC – VIEGLI NOMALDĪTIES UN KĻŪT PAR UPURI

- Uzbrukums vidēji paliek nepamanīts **200+ dienas** (ENISA)
- Nopietna kiberincidenta izmaksas var pārsniegt **1,5+ milj. €** (tiešie un netiešie zaudējumi)
- Reputācijas risks – **klientu uzticības zaudēšana**
- Pastiprināts regulējums: **sodi** par NKDL/DORA/GDPR pārkāpumiem un tiesvedības izmaksas.



SOC TEHNOLOĢISKAIS PAMATS



SOC KĀ “DROŠĪBAS APDROŠINĀŠANA”

- Samazina zaudējumu risku
- Prognozējamas izmaksas un investīcijas
- Biznesa nepārtrauktība – samazina uzņēmuma dīkstāvi un reputācijas zaudējumu



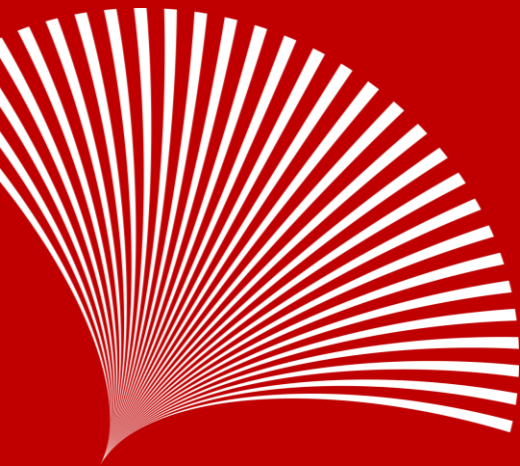


LATVIJAS VALSTS
RADIO UN TELEVĪZIJAS CENTRS



PALDIES PAR UZMANĪBU!

ATBILDĪBA / ATTĪSTĪBA / ATVĒRTĪBA
Droša, jaudīga un iekļaujoša digitālā Latvija.



JAUTĀJUMI

