



Automatizēts informāciju sistēmas DROŠĪBAS
RISINĀJUMS maziem un vidējiem datortīkliem

Raimonds Bricis



PEDAB

Dienas kārtība

- Esošā situācija
- Kas ir Drošības Monitorings un Ko tas dara?
- Mūsu pieredze
- Ko mēs piedāvājam
- Demo

Esošā situācija

- Apdraudējumu skaits nepārtraukti pieaug
- Grūtības identificēt apdraudējumu avotus
- Drošība nav iekārtu ražotāju prioritāte
- Atbildība palielinās (likumi, regulas)

Organizāciju pamata esošās drošības sistēmas

TĪKLS

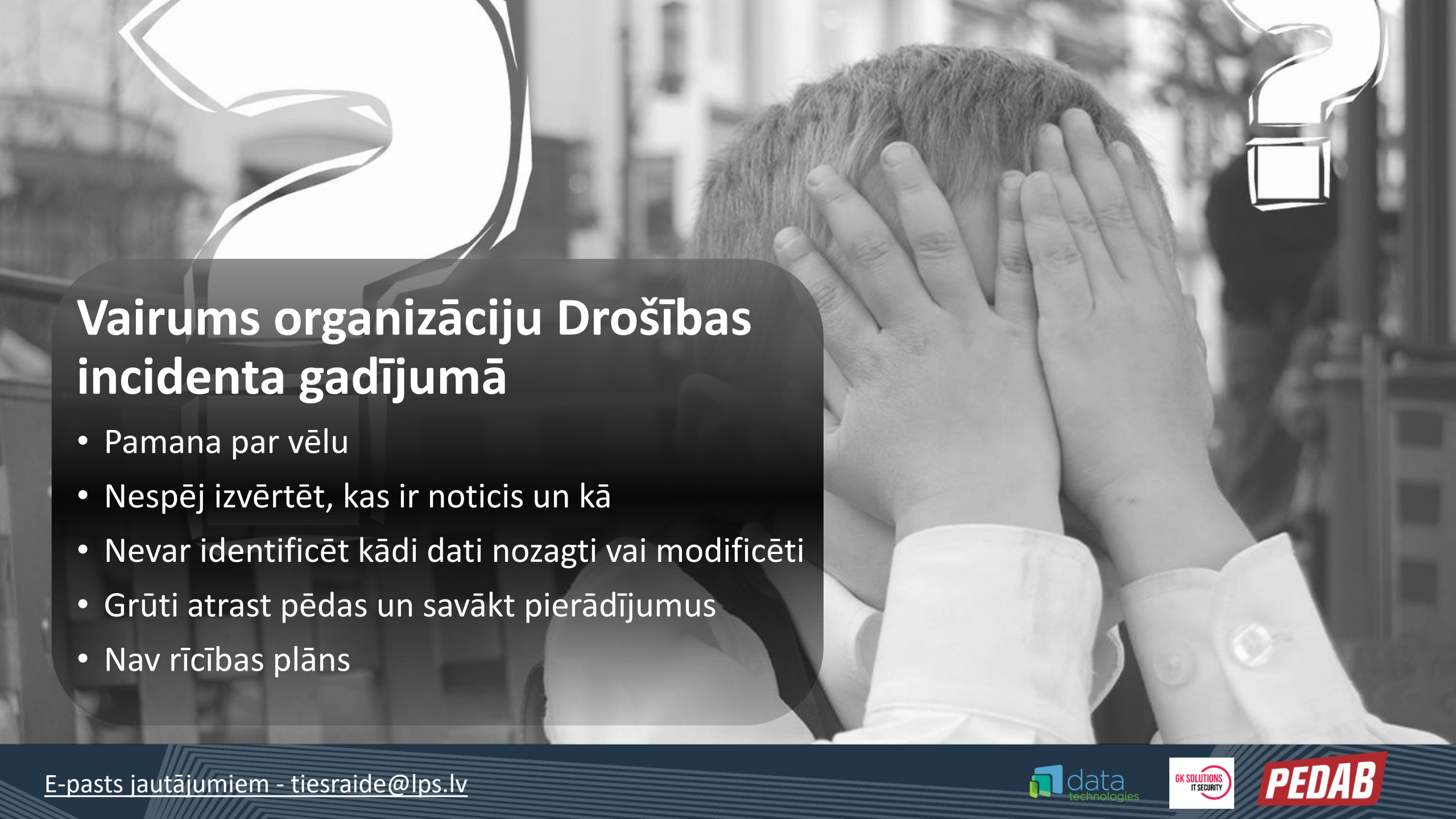
Ugunsmūris / Jaunās paaudzes ugunsmūris

PIEKĻUVE

Lietotāja vārds & Parole / Daudzfaktoru autentifikācija

DATORI
TELEFONI

Antivīruss / Ļaunatūras aizsardzība un «End Point Management»



Vairums organizāciju Drošības incidenta gadījumā

- Pamana par vēlu
- Nespēj izvērtēt, kas ir noticis un kā
- Nevar identificēt kādi dati nozagti vai modificēti
- Grūti atrast pēdas un savākt pierādījumus
- Nav rīcības plāns

Cisco ACS-User Authentication Success

	Device Address	User Name	Account Type	Authentication Type	NAS Address	NAS Port	Destination Address	Destination
01:16 PM	10.60.1.240	trav	Internal Users	Radius	10.60.1.240	129		
02:19:36 PM	10.60.1.240	Racidbkupusr	Meggitt-LDAP	Radius	10.212.9.250	2	10.212.9.140	1645
02:18:35 PM	10.60.1.240	Racidbkupusr	Meggitt-LDAP	Radius	10.212.9.250	1	10.212.9.140	1645
02:13:16 PM	10.60.1.240	trav	Internal Users	Radius	10.60.1.240	129		
02:39:56 PM	10.60.1.240	Racidbkupusr	Meggitt-LDAP	Radius	10.212.9.250	1	10.212.9.140	1645
02:14:56 PM	10.60.1.240	Racidbkupusr	Meggitt-LDAP	Radius	10.212.9.250	2	10.212.9.140	1645
01:49:36 PM	10.60.1.240	Racidbkupusr	Meggitt-LDAP	Radius	10.212.9.250	1	10.212.9.140	1645
01:19:36 PM	10.60.1.240	trav	Internal Users	Radius	10.60.1.240	129		
09:39:56 PM	10.60.1.240	Racidbkupusr	Meggitt-LDAP	Radius	10.212.9.250	2	10.212.9.140	1645
04:19:26 PM	10.60.1.240	Racidbkupusr	Meggitt-LDAP	Radius	10.212.9.250	1	10.212.9.140	1645
01:17:33 PM	10.60.1.240	trav	Internal Users	Radius	10.60.1.240	129		
01:09:36 PM	10.60.1.240	Racidbkupusr	Meggitt-LDAP	Radius	10.212.9.250	2	10.212.9.140	1645
01:06:56 PM	10.60.1.240	Racidbkupusr	Meggitt-LDAP	Radius	10.212.9.250	1	10.212.9.140	1645
01:06:56 PM	10.60.1.240	Racidbkupusr	Meggitt-LDAP	Radius	10.212.9.250	2	10.212.9.140	1645
01:06:56 PM	10.60.1.240	trav	Internal Users	Radius	10.60.1.240	129		
01:06:56 PM	10.60.1.240	trav	Internal Users	Radius	10.60.1.240	129		
01:06:56 PM	10.60.1.240	Racidbkupusr	Meggitt-LDAP	Radius	10.212.9.250	2	10.212.9.140	1645
01:06:56 PM	10.60.1.240	Racidbkupusr	Meggitt-LDAP	Radius	10.212.9.250	1	10.212.9.140	1645
01:06:56 PM	10.60.1.240	Racidbkupusr	Meggitt-LDAP	Radius	10.212.9.250	1	10.212.9.140	1645
01:06:56 PM	10.60.1.240	Racidbkupusr	Meggitt-LDAP	Radius	10.212.9.250	2	10.212.9.140	1645

	Facility	Severity	Process	Message
10:28	System	Information	void	10 YODA\verno Document
10:44:53	System	Information	w32time	7036 The Syslogserver serv
10:44:53	System	Information	w3svc	7035 GONZD\verno The S
10:44:53	System	Information	win32k	(root) CMD (run-parts /etc/c
10:44:53	Clock	Information	xinetd	
11:03:26	Application	Information	gonzo	101 wuaucft (432) The data
11:03:26	Application	Information	gonzo	103 wuaueng.dll (432) SUS
11:03:22	Application	Information	gonzo	102 wuaueng.dll (432) SUS
11:03:22	Application	Information	gonzo	100 wuaucft (432) The data
11:03:26	Security	Information	gonzo	680 NT AUTHORITY\SY
11:03:26	Clock	Information	MissPiggy	(root) CMD (run-parts /etc/c
11:03:26	Application	Information	yoda	17055 YODA\Administrato
11:03:26	Clock	Notice	MissPiggy	Normal exit (1 jobs run)
11:03:26	Clock	Notice	MissPiggy	Job `cron.daily' terminated
11:03:26	Clock	Notice	MissPiggy	Updated timestamp for job `
11:03:26	Mail	Information	MissPiggy	iAQCmHuU007636: to=root
11:03:26	Mail	Information	MissPiggy	iAQCmHuU007636: from=r
11:03:26	Clock	Information	MissPiggy	(root) CMD (run-parts /etc/c
11:03:26	Clock	Information	MissPiggy	(root) CMD (run-parts /etc/c
11:03:26	Clock	Notice	MissPiggy	Job `cron.daily' started
11:03:26	System	Information	yoda	10 YODA\mari Document
11:03:26	Application	Information	gonzo	101 wuaucft (2860) The dat
11:03:26	Application	Information	gonzo	103 wuaueng.dll (2860) SU
11:03:26	System	Error	gonzo	7023 The Computer Browse
11:03:26	System	Information	gonzo	7036 The Computer Browse
11:03:26	Clock	Information	MissPiggy	(root) CMD (run-parts /etc/c
11:03:26	System	Information	gonzo	7036 The Network Location
11:03:26	System	Information	gonzo	7035 NT AUTHORITY\SY

Visas sistēmas viedo notikumu žurnālfailus (log file)

Tos ir sarežģīti lasīt

Neviens tos nelasa

Kas ir Drošības Monitorings un Ko tas dara?



Informācijas savākšana
un uzglabāšana

Informācijas korelācija
un analīze

Prioretizēšana
Trauksmes ziņojumi
Notikumu izmeklēšana

Drošības monitorings SIEM

Log
Pārvaldība

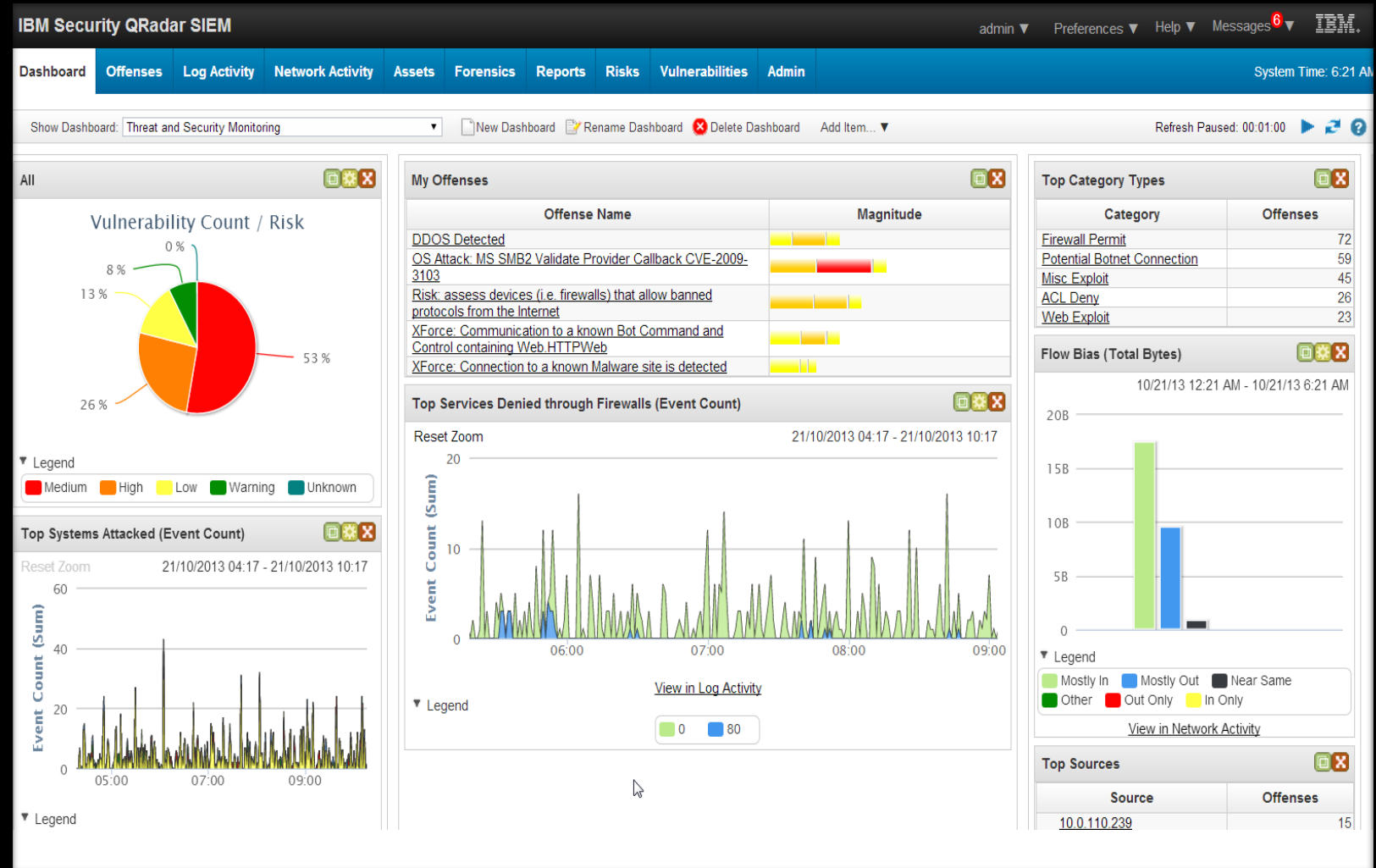
Drošības notikumu
uzraudzība

Tīkla notikumu
uzraudzība

Risku pārvaldība

Ievainojumu
pārvaldība

Padziļināta tīkla
notikumu izmeklēšana



Mūsu pieredze!

- Neeksistējošu kontu izmantošana iekšējās IT sistēmās
- Darbinieku kontu, kuri vairs nestrādā izmantošana
- Neautorizēta piekļuve sistēmām, kurām lietotājam jābūt liegtai pieejai
- IT sistēmas BotNet tīkla sastāvā
- Paroļu uzlaušanas mēģinājumi
- Neautorizētu IT sistēmu parādīšanās korporatīvajā tīklā
- Liela datu apjoma izsūtīšana ārpus uzņēmuma korporatīvā tīkla
- AWS/Azure Cloud resursu izmantošana privātām vajadzībām
- Datu centra resursi izmantoti Bitcoin fermu uzturēšanai

Ministru kabineta noteikumi Nr. 442

- Lietotāju kontu pārvaldība
- Ievainojamību un atjauninājumu pārvaldīšana
- Kontu pārvaldība paaugstinātai drošībai
- Attālinātas piekļuves monitorings
- Log datu uzglabāšanas prasības
- Incidentu pārraudzība
- Sistēmas apdraudējumu novērtējums
- Uzbrukumu simulēšana ar Risk Manager
- Veikto pasākumu lietderības (Atkārtota V/A skanēšana, Salīdzinošās atskaites (delta) Riska novērtējuma (scoring) samazināšanās)



Kā varam palīdzēt?



Došības Monitorings SIEM

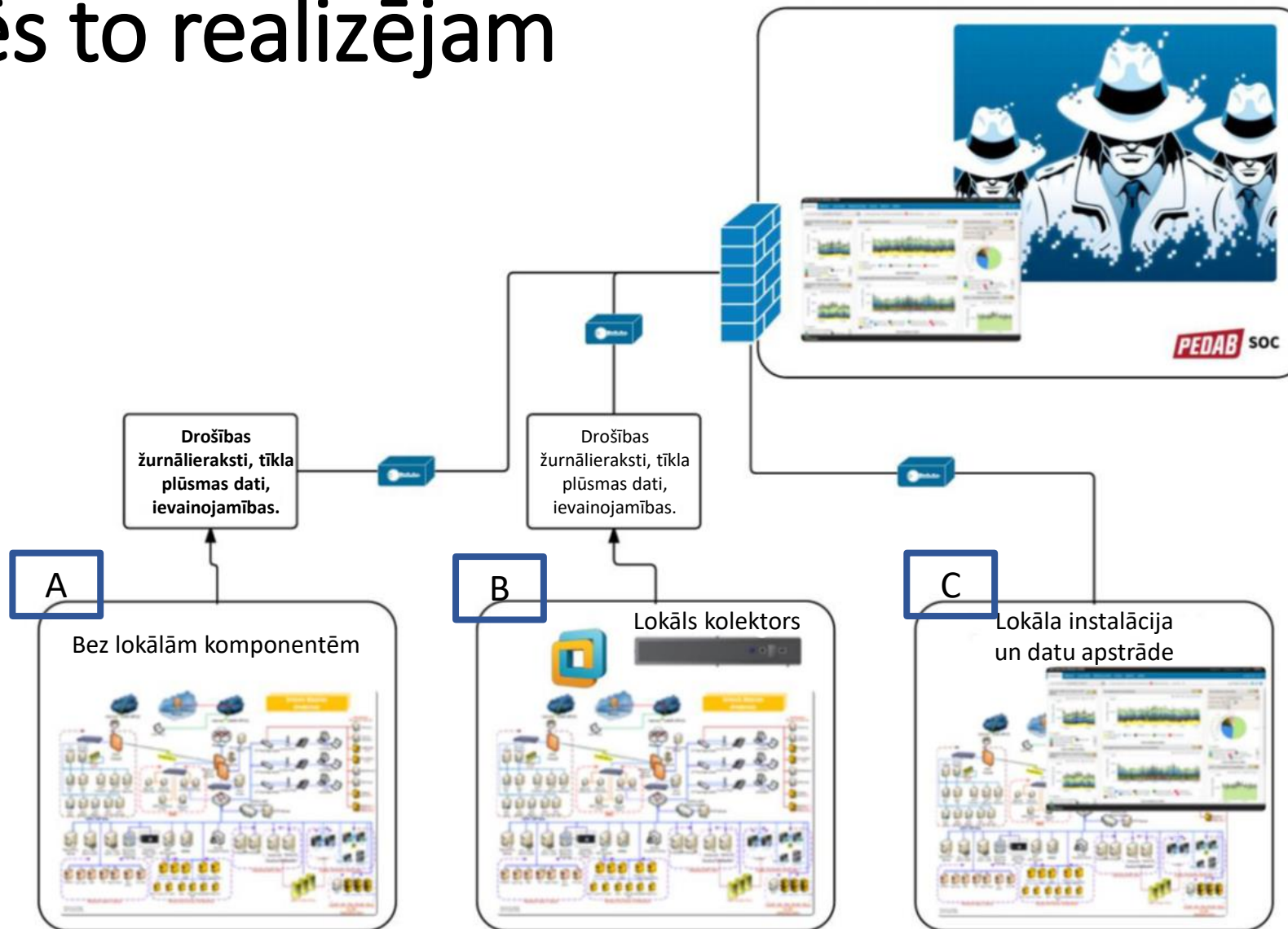
- Automatizēts IT drošības uzraudzības risinājums
- Reāllaika skatījums uz drošības notikumiem uzņēmuma sistēmās
- Visi notikumi tiek glabāti drošā un pārskatāmā veidā
- Apdraudējumu atpazīšana un prioritizēšana
- Trauksmes ziņojumi par sliktākajiem notikumiem
- Automatizētas sākotnējās darbības kaitējuma samazināšanai

Došības Eksperta Pakalpojums

- Sertificēts IT drošības eksperts, uzrauga uzņēmuma IT sistēmu drošību
- Reāllaika skatījums uz drošības notikumiem uzņēmuma sistēmās
- Visi notikumi tiek glabāti drošā un pārskatāmā veidā
- Apdraudējumu atpazīšana un prioritizēšana
- Kritiskos gadījumos eksperts sazinās ar klientu
- Automatizētas sākotnējās darbības kaitējuma samazināšanai



Kā mēs to realizējam



Jūsu jautājumi

[E-pasts jautājumiem - tiesraide@lps.lv](mailto:tiesraide@lps.lv)



DEMO >>>

Sazinies ar mums

raimonds.bricis@pedab.lv / +371 26361249

www.pedab.lv



Paldies!