Automatizēts informāciju sistēmas DROŠĪBAS RISINĀJUMS maziem un vidējiem datortīkliem

Raimonds Bricis

data technologies

GK SOLUTIONS IT SECURITY

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)

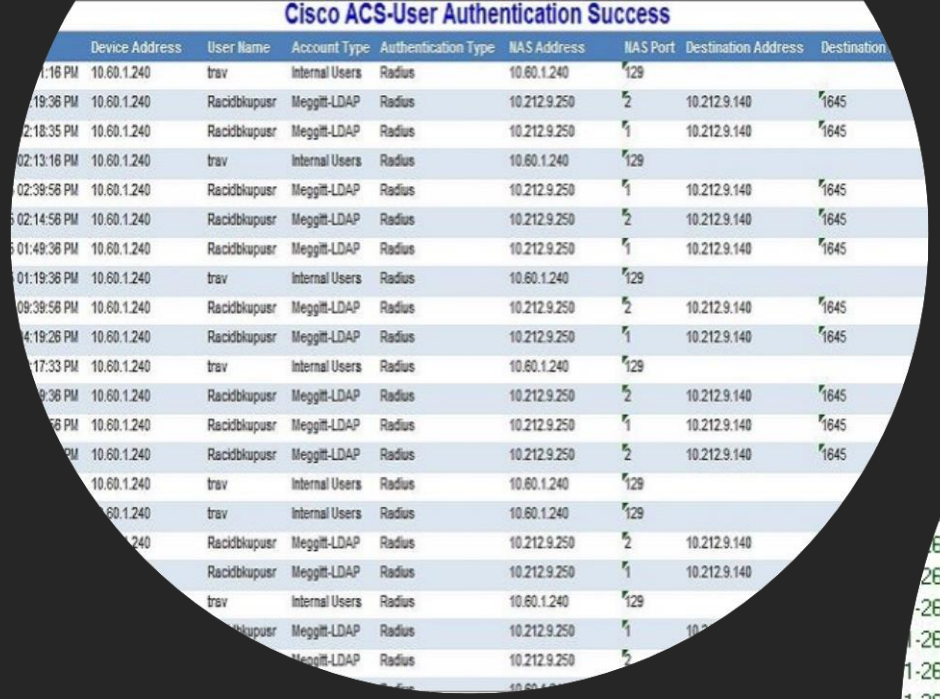
E-pasts jautājumiem - tiesraide@lps.lv

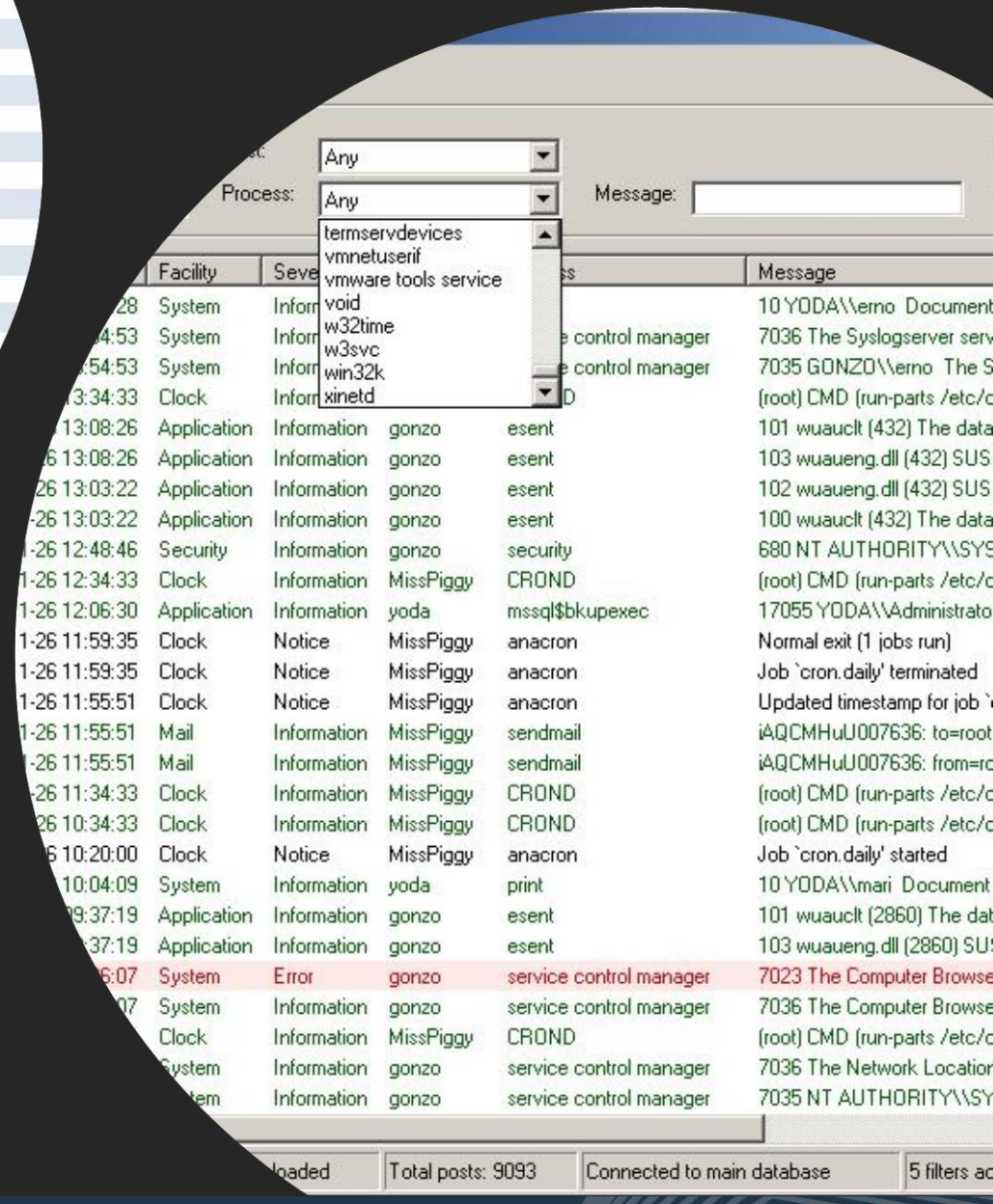
Organizāciju pamata esošās drošības sistēmas

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





Visas sistēmas viedo notikumu žurnālfailus (log file)

~~Tos ir sarežģīti lasīt~~

Neviens tos nelasa

Kas ir Drošības Monitorings un Ko tas dara?

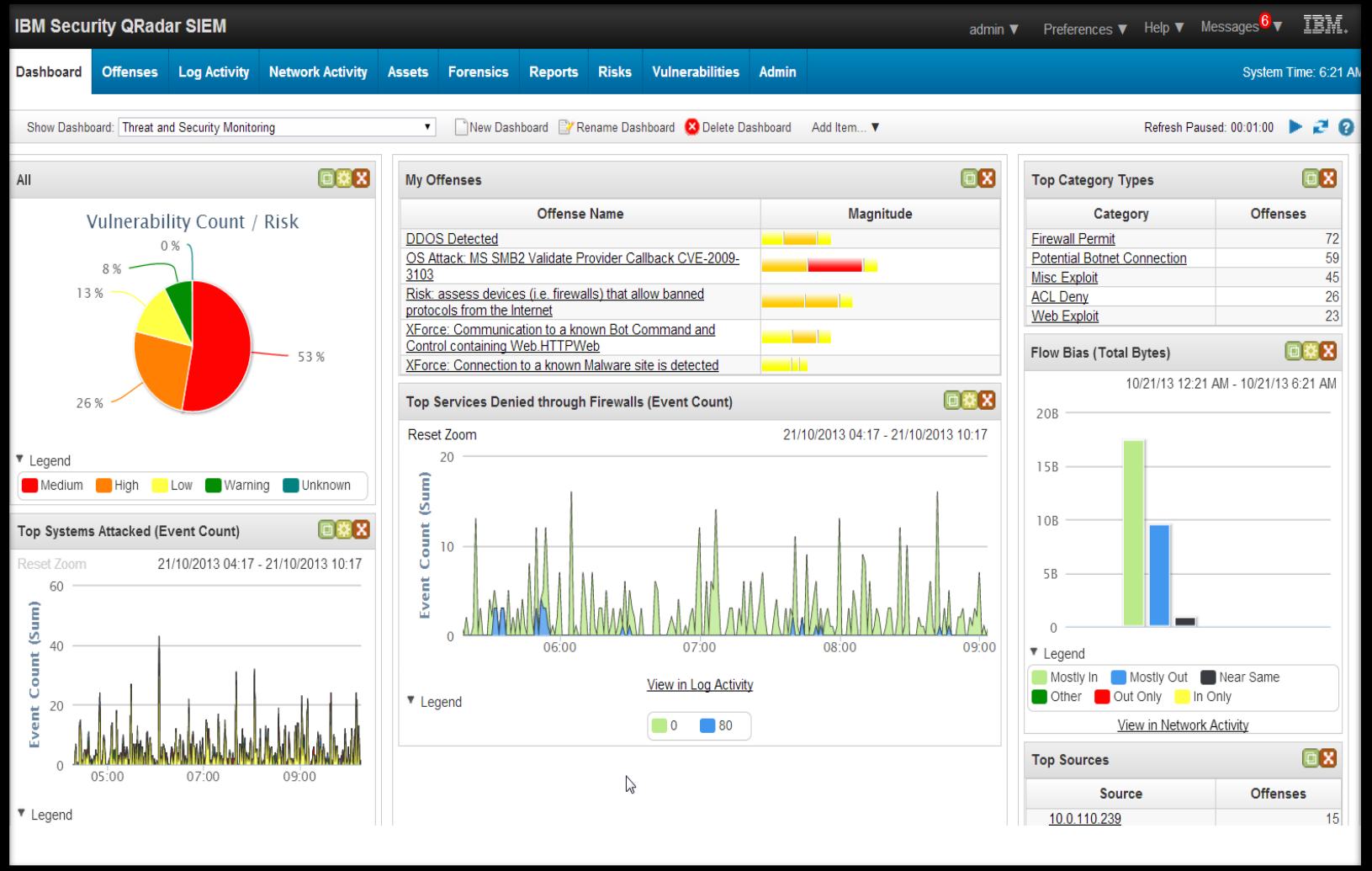
Informācijas savākšana un uzglabāšana

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



E-pasts jautājumiem - tiesraide@lps.lv

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

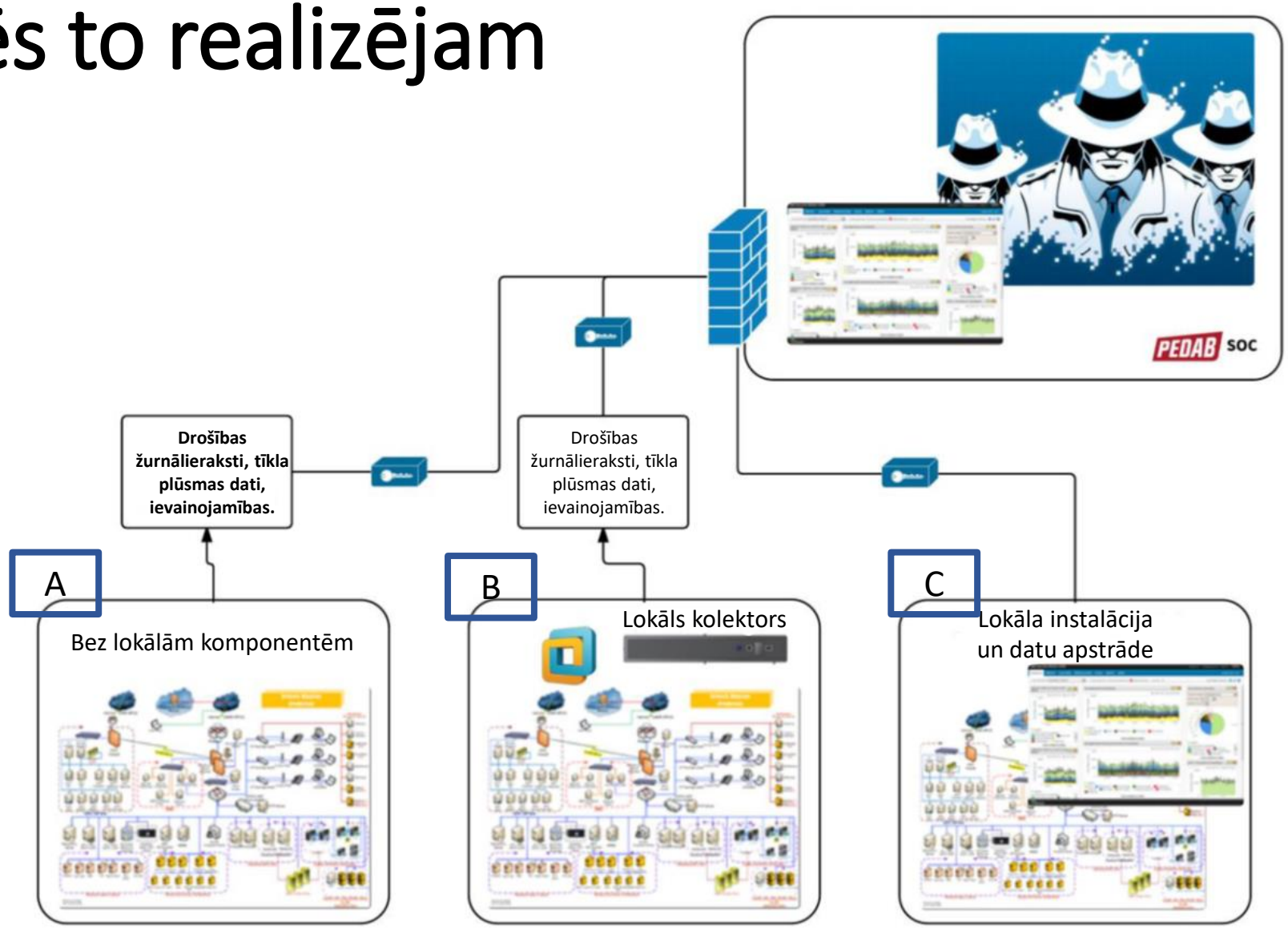
- Automatizēts IT drošības uzraudzības risinājums
- Reāllaika skatījums uz drošības notikumiem uzņēmuma sistēmās
- Visi notikumi tiek glabāti drošā un pārskatāmā veidā
- Apdraudējumu atpazīšana un prioritizēšana
- Trauksmes ziņojumi par sliktākajiem notikumiem
- Automatizētas sākotnējās darbības kaitējuma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

E-pasts jautājumiem - tiesraide@lps.lv

Kā mēs to realizējam



Jūsu jautājumi

E-pasts jautājumiem - tiesraide@lps.lv


DEMO »

Sazinies ar mums

raimonds.bricis@pedab.lv / +371 26361249
www.pedab.lv

Paldies!