

Kas nepieciešams Modernai drošībai?

2023-09-26

Iepazīsimies!

- Kārlis Bergmanis
- IT kopš 2007
- Pre-sales, Red team, Blue team, All-Star team
- Evolution Latvija informācijas drošības speciālists
- Moto «This is fine»



Mērķis: saprast principus

**Trendi un kā
tiem tuvojies**

**Bez cilvēkiem
pat tramvajs
nekustas**

**Dati ir visa
centrā**

**Struktūra nāk
pirmā**



Mainīgie trendi, Paliekošie trendi

Skatoties vēsturē

- BYOD bija nākotne – bet tomēr uzņēmumu iekārtas paliek
- Mākonis bija nākotne – bet tomēr mums ir arī serveri
- All-Remote bija nākotne – bet tomēr mēs reizēm tiekamies ofisā
- AI ir nākotne...



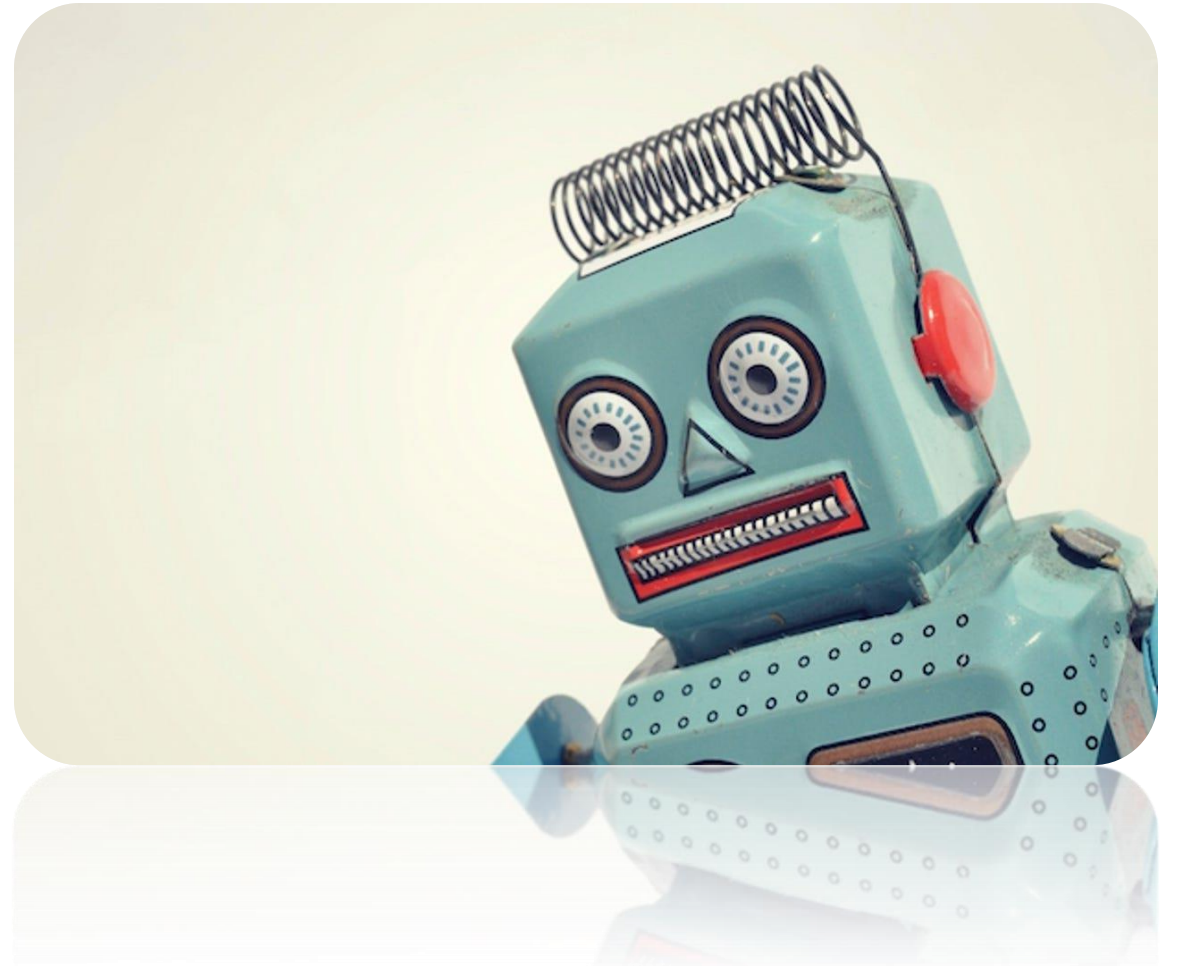
Tātad?

- Šķipsniņa sāls
- Noteikta tehnoloģija, noteikta programma - nē



Kas ir īstie trendi

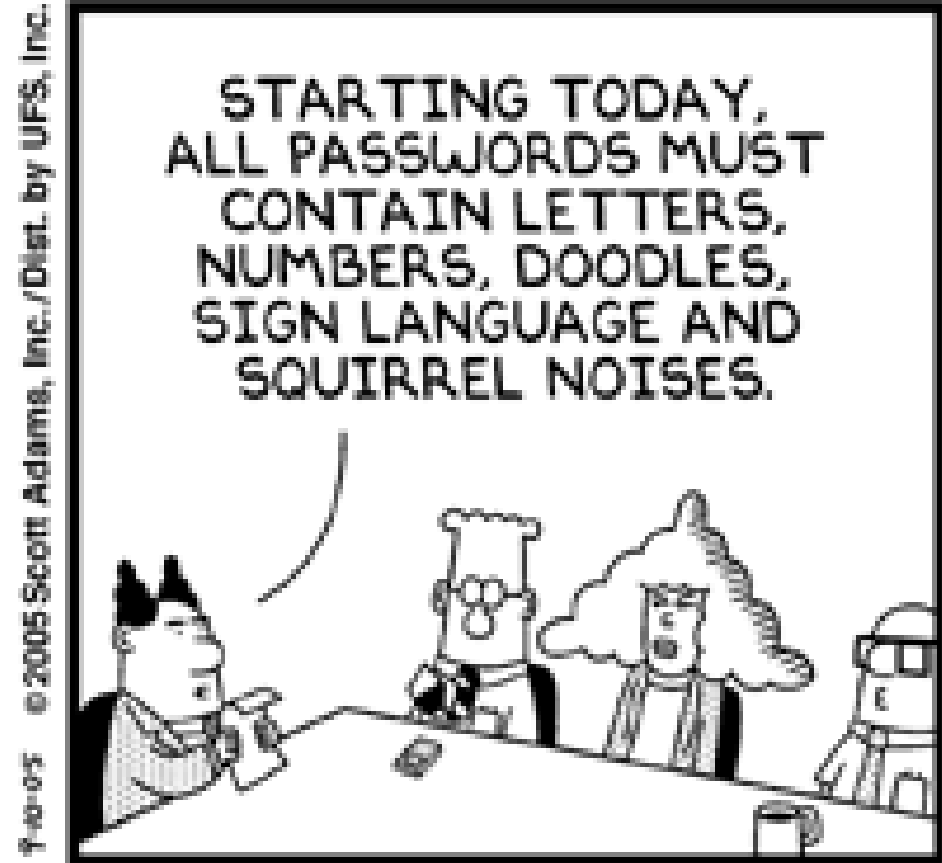
- GDPR
- NIS / NIS2
- Vienotā pieteikšanās
- eID



Cilvēks ir visa
atslēga

Kur ņemt ideālus darbiniekus?

- Ja viņi izlasītu pamācības
- Ja klausītu, ko saka
- Un vispār – darba laikā strādātu
- Un domātu līdzī, vai ne...



Jāiesaistās ir visiem

- Drošībai jā sākas no augšas
- C līmenis, direktori, sektoru vadītāji
- IT nodaļa, IT vadītāji un administratori
- Tikai tad - lietotāji



Vai tiešām viņiem to vajag?*

- Grāmatvedis nāk uz darbu rēķināt
- HR nāk uz darbu pieņemt kādu darbā
- Vai viņiem būtu jāzina kaut kas par kiberdrošību?
- Kāpēc?



Jā

- IT sen nav tikai darba lieta, vai ne?
- Saprātīgas prasības



Dati ir visa centrā

Iekārtu nozīme mazinās

- Ja viss ir izdarīts pareizi – iekārta tiešām ir mazsvarīga
- Ir pieejami mehānismi iekārtu atkopšanai
- Informācija ir tur ārā



Ko grib hakeri?

- Iegūt informāciju un nopelnīt ar tās nepublicēšanu
- Nošifrēt serverus / datorus un nopelnīt par to atšifrēšanu
- Veikt DDoS un nopelnīt par tā apturēšanu
- Izlikties par Adminu vai CEO un...



Tātad

- Dati, dati un dati
- Antivīrusi un ugunsmūri, jā
- Bet arī
- DLP, IRM, PAM, VPN, MFA



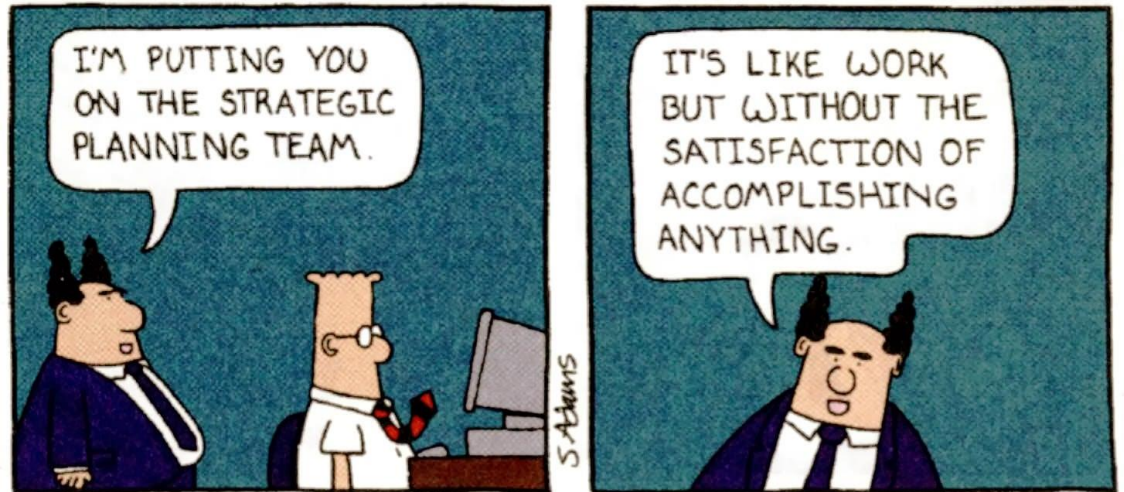
Kāpēc?
Kāpēc?
Kāpēc?

Tā ir māja*



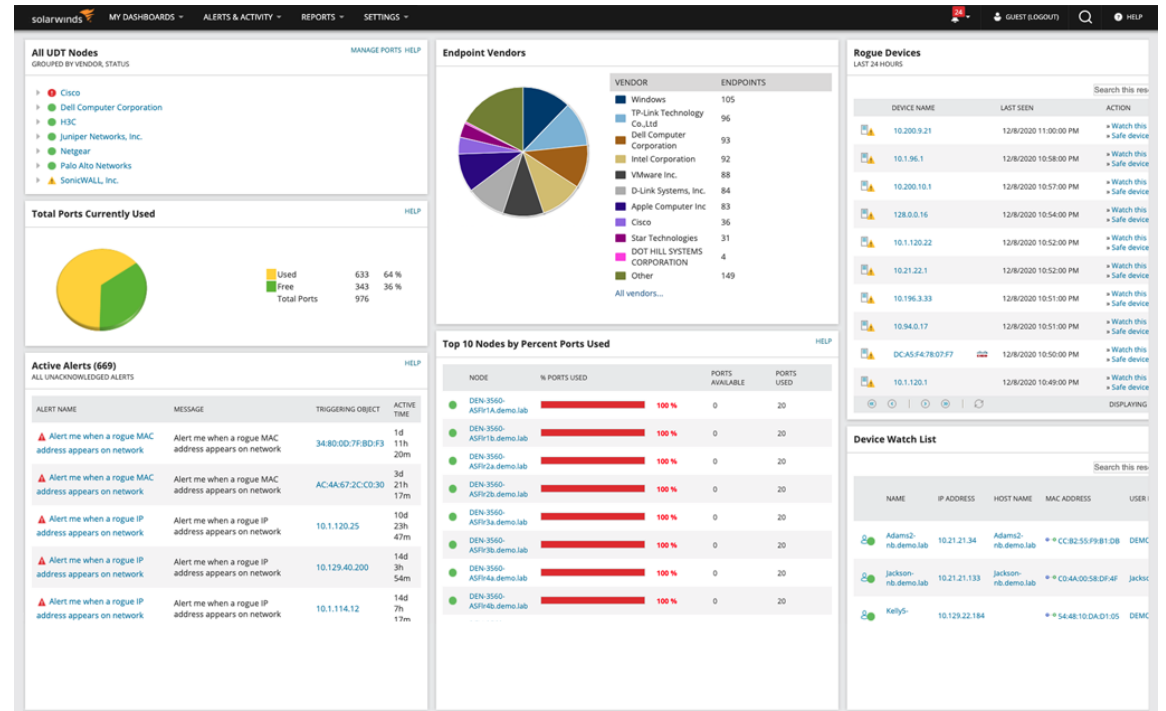
Īsta kiberdrošība

- Uzinstalēt kaut ko ir īsts darbs
- Rakstīt politikas ir vienkārši laika patēriņš
- Nejauša kiberdrošība



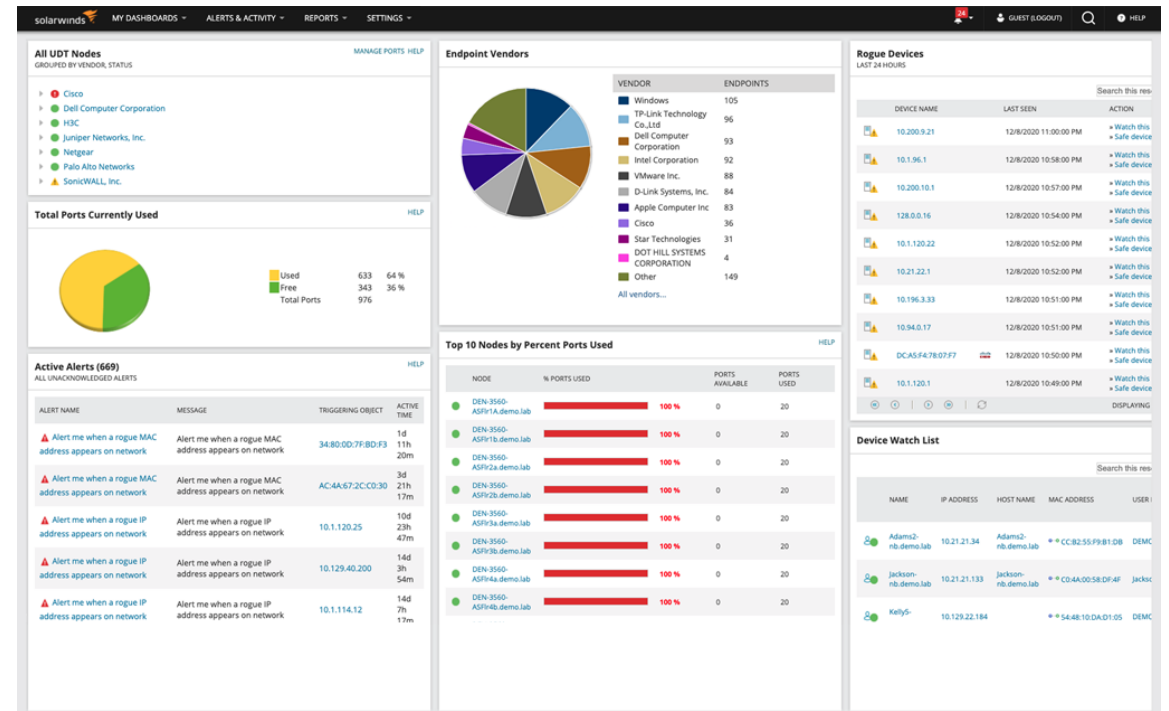
Mazs uzņēmums

- Inventarizācija – kas mums pieder
- Cik mums darbinieku
- Ko viņi dara



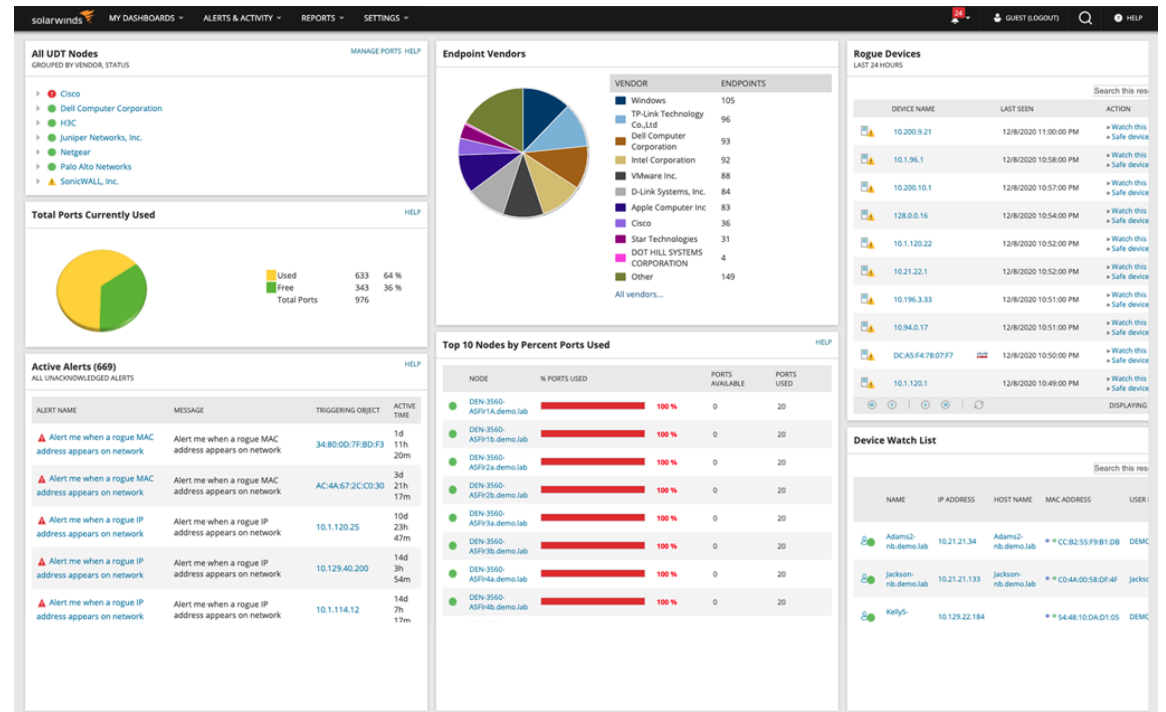
Vidējs uzņēmums

- Vienota konfigurācija
- Politikas
- Procedūras
- Ja ne 24/7, tad 8/5 uzraudzība



Lielie uzņēmumi

- ISO27001*
- Pienākumu atdalīšana



Ceļavārdi

Kopsavilkums

- Apmācības : Procedūras : Kontroles
veselīgā līdzsvarā
- Jāzina, ko sargāt – un no kā
- Drošība ir kopīga lieta



**DON'T
PANIC**



Evolution
Engineering



**ACCELERATING
EVOLUTION**