Draudu simulācija - ieguvums par saprātīgu cenu

Andris Medjānis

CERT.LV
Kiberincidentu novēršanas institūcija

Rīga, 2024

Plāns

- Kas ir draudu simulācija un mērķis

- Ieguvumi organizācijai
- Ar ko sākt un kādēļ

- Kādēļ ‘‘saprātīga cena’’

CERT.LV

Simulācija visam

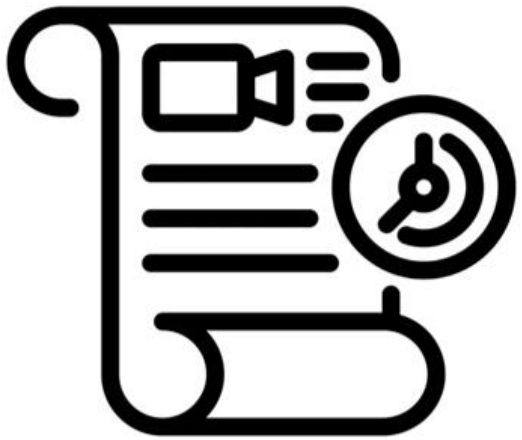
- Datu atjaunošana no rezerves kopijas
- Datora pārinstalēšana ne tikai vīrusu, bet atjauninājuma bojājuma dēļ (+liet. faili, programmas)
- Interneta pieslēguma traucējumi (alternat.piesl.)
- Klēpjdatora bojājums (nomaiņas ātrums)
- Daudzfaktoru lietotnes problēmas (MFA plāns B)
- Ir sistēmas, procedūras, sertifikācijas; trūkst prakses

CERT.LV

Salīdzinājumam

Draudu Simulācija ir kā mācību ugunsgrēka trauksme:

Procedūras,Procesi, Rīki, Rīcība, Secinājumi



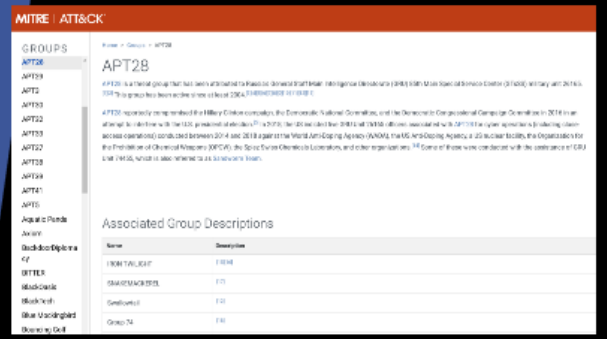
Minimālās prasības – detektori, žurnāli + analīze, personāls

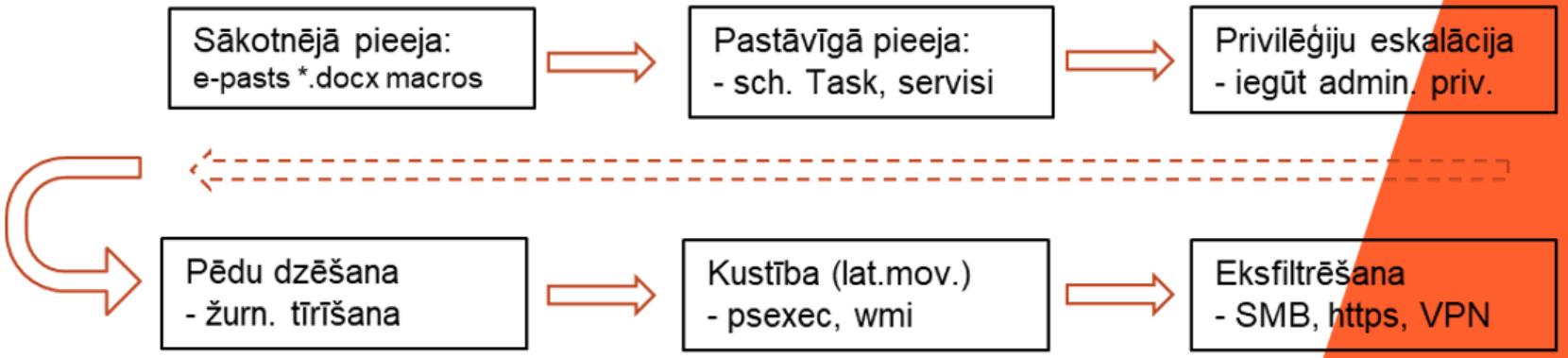
Kas ir draudu simulācija

- Draudu simulācija – viena no kiberdrošības novērtējuma metodēm
- Mērķis: pārbaudīt un uzlabot organizācijas drošības sistēmas, kontroles, procesus un procedūras

  - iekļaujot uzbrucēju taktiku, tehniku un procedūras (TTP)
  - iekļaujot uzbrucēja profilu (APT28, Turla, Blizzard u.c.)

- pamats: MITRE ATT&CK ietvars
- kā sistēmās uzvedas uzbrucējs, viņa rīcība un rīki





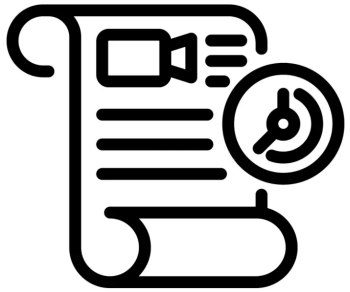
CERT.LV

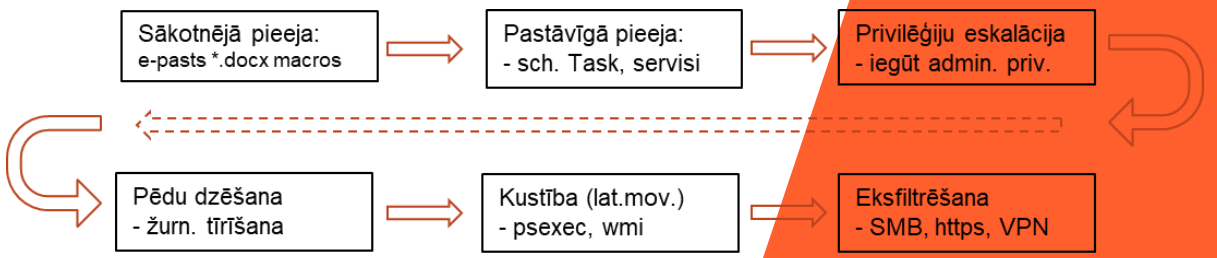
Būtiski par draudu simulāciju

Draudu Simulācija nav: ✗

- Red Team aktivitātes (kontrolētie uzbrukumi)
- Draudu medības
- Ielaušanās testi (pen test)

Draudu Simulācija ir iepriekš sagatavots uzbrukums: ✓





Draudu simulācijas ieguvumi

- Aktīvo drošības sistēmu pārbaude gala iekārtās
- Procedūru darbības pārbaude praksē
- Speciālistu treniņš
- Trauksmes un ziņojumu, signālu pārbaude
- Trūkumu atklāšana un novēršana

- Jebkuri citi sasniegumi procesa gaitā

‘‘Ieguvums par saprātīgu cenu’’

- Minimālas pakalpojuma saņēmēja izmaksas
  - Viena testa iekārta (Windows)
  - Personāla laiks
- Ieguvums pārsniegs ieguldīto

Būsim sagatavoti un droši!

PALDIES!

Jautājumi? Komentāri?