CERT.LV

Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Incident Response pamati

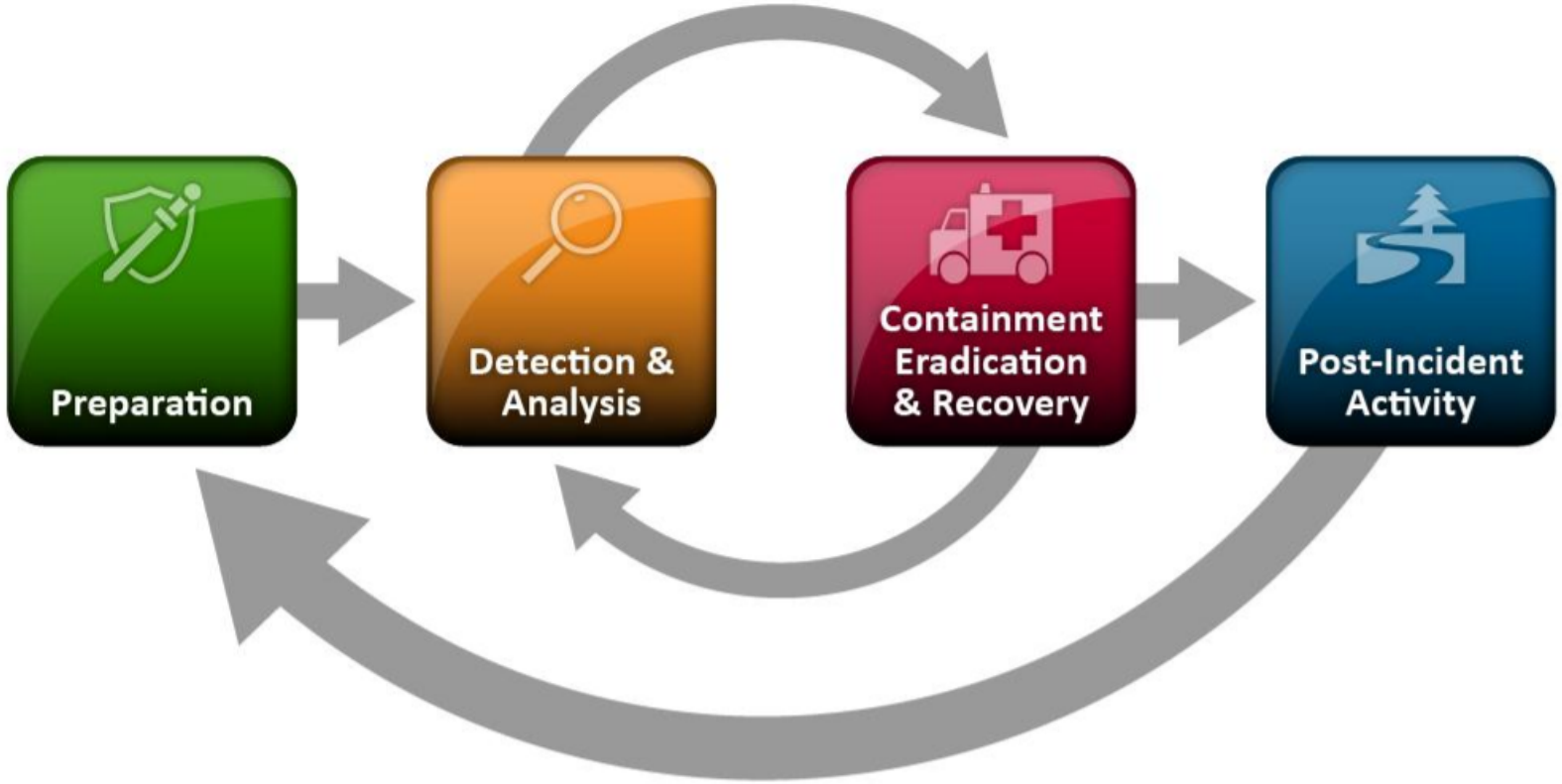
Esi Drošs, 10.12.2020

Andrejs Konstantinovs
andrejs@cert.lv

Prezentācijas mērķi

- Kā atpazīt kiberincidentu?
- Kādus cilvēkus iesaistīt incidenta risināšanā?
- Kad griezties uz CERT.LV?
- Kā saglabāt pierādījumus kriminalistikas analīzei?

Incidentu apstrādes modelis



Sagatavošanās stadija

- ✓ Incidenta risināšanai nepieciešamās personas, to 24/7 kontakti:
  - Atbildīgais par incidentu kopumā
  - IT administratori, atbalsta darbinieki
- ✓ Komunikācijas kanāli (epasti, čats, telefoni)
- ✓ Datu nesēji & programmatūra pierādījumu vākšanai
- ✓ Rezerves datori (“known-good”)
- ✓ Rezerves kopijas
- ✓ CERT.LV kontakti (https://cert.lv/lv/kontakti)

Sagatavošanās stadija (turp.)

- ✓ Infrastruktūras karte
- ✓ Lietoto iekārtu & programmatūras sarkasts
- ✓ “Zelta attēli” serveriem & darbstacijām
- ✓ Centralizēta žurnālfailu vākšana un apstrāde
- ✓ Monitorings, brīdinājumi, anomāliju atpazīšana
- ✓ Tīkla un gala iekārtu drošības risinājumi
- ✓ Darbinieku izglītošana

Incidenta atpazīšana

Iekšējie ziņojumu avoti:

- Monitoringa sistēmas / SIEM
- AV / EDR risinājumi
- Ziņojumi no darbiniekiem
- Proaktīva draudu atpazīšana
- Red-team vingrinājumi

Ārējie ziņojumu avoti:

- Informācija no partneriem/klientiem
- Brīdinājumi no IPS
- Brīdinājumi no CERT.LV
- Responsible disclosure
- Avīzes, mēdiji, …

Pierādījumu vākšana & analīze

- ✓ Ātrums & precizitāte
- ✓ Jāņem vērā konkrētā incidenta konteksts, triāža
- ✓ Mērķi:
  - Savākt pierādījumus
  - Noskaidrot *incident scope*
  - Nepieļaut jaunu sistēmu inficēšanos

Operatīvā atmiņa

- ✓ Virtualizācijas gadījumā, attēli jāveido no virtualizācijas hosta
- ✓ Veidojot attēlus no *live* sistēmas ar >2GB RAM – data smear
- ✓ *Crash dumps* – labāka atomicitāte, bet izvairīšanās risks
- ✓ Programmas izvēle:
  - Ieteicams open-source (WinPMem)
  - Vēlams rakstīt uz ārējo nesēju

Datu nesēji

- ✓ Ja diski nav šifrēti, visdrošāk saglabāt pierādījumus:
  - atslēdzot elektrību
  - nododot izmeklēšanai oriģinālus, vai to kopijas, kas veidotas no drošas vides
- ✓ Laižot kriminalistikas programmas no *live* sistēmas – risks pazaudēt datus
- ✓ Pieslēdzot inficētos diskus citām darbstacijām – risks inficēt arī tās

Žurnālfaili

- ✓ Var nākt no:
  - disku analīzes
  - centralizētām sistēmām
  - tīkla iekārtām
  - mākoņpakalpojumiem
- ✓ Parasti var veikt tie paši darbinieki, kas apkalpo attiecīgās sistēmas
- ✓ Pēc noklusējuma vāktā informācija bieži vien ir ierobežota

Ierobežošanas / izskaušanas fāze

- ✓ Sākumā jāidentificē skartās sistēmas
- ✓ Skartās sistēmas:
  - Pāristalēšana
  - Atjaunošana no rezerves kopijām
- ✓ Jāpasargā neskartās sistēmas
- ✓ Papildus monitorings & redzamība

Pēc-incidenta uzdevumi

- ✓ Faktu & veikto darbību apokopšana, gala atskaites veidošana
- ✓ Apziņošana:
  - Vadība
  - Darbinieki, partneri, klienti
  - Citas skartās puses
  - CERT.LV
- ✓ Tiesībsargājošās iestādes