Hogyan SOC-ol egy CSIRT?

2023. május 25

Marsi Tamás

Mégis hogyan?

A válasz, ...

- ...sehogy
- A SOC nem CSIRT!
- Pont.

- Köszönöm a figyelmet!

Mi egy SOC dolga?

- Eseményeket észlel
- Eseményekből incidenseket eszkalál
- Incidenseket vizsgál ki
- Biztonsági fenyegetéseket keres
- Ha szükséges, beavatkozik
- TEHÁT egy vagy több rendszer biztonságát erősíti
- Még jobban tehát: emberek ülnek nagy monitorok előtt

Mi egy CSIRT dolga?

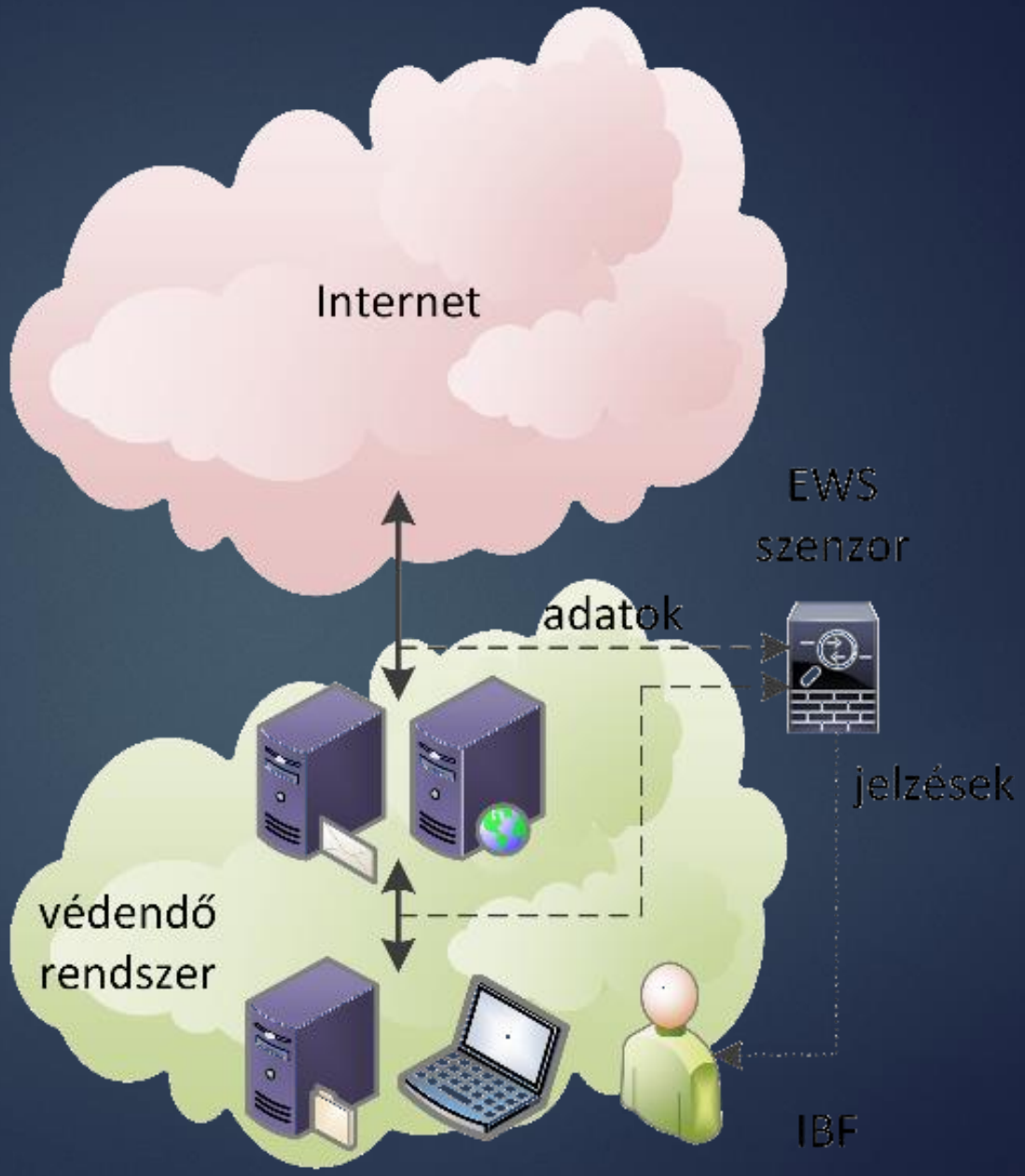
- Koordinál, kivizsgál
- Információt gyűjt és oszt meg
- Trendeket figyel
- Passzívan erősíti a kiberbiztonságot
- TEHÁT egy szektor vagy ország kiberbiztonságát erősíti
- Még jobban tehát: emberek ülnek nagy monitorok előtt

Tehát?

NKI SOC(szerű) funkciói

- EWS
- Honeypot
- ASR
- Rendes SOC
- CTI
- Threat hunting
- Forensic és IH

EWS


Internet
EWS
szenzor
adatok
jelzések
védendő
rendszer
IBF

Honeypot

ASR

AUTOMATIZÁLT
SÉRÜLÉKENYSÉGVIZSGÁLATI
RENDSZER

Rendes SOC

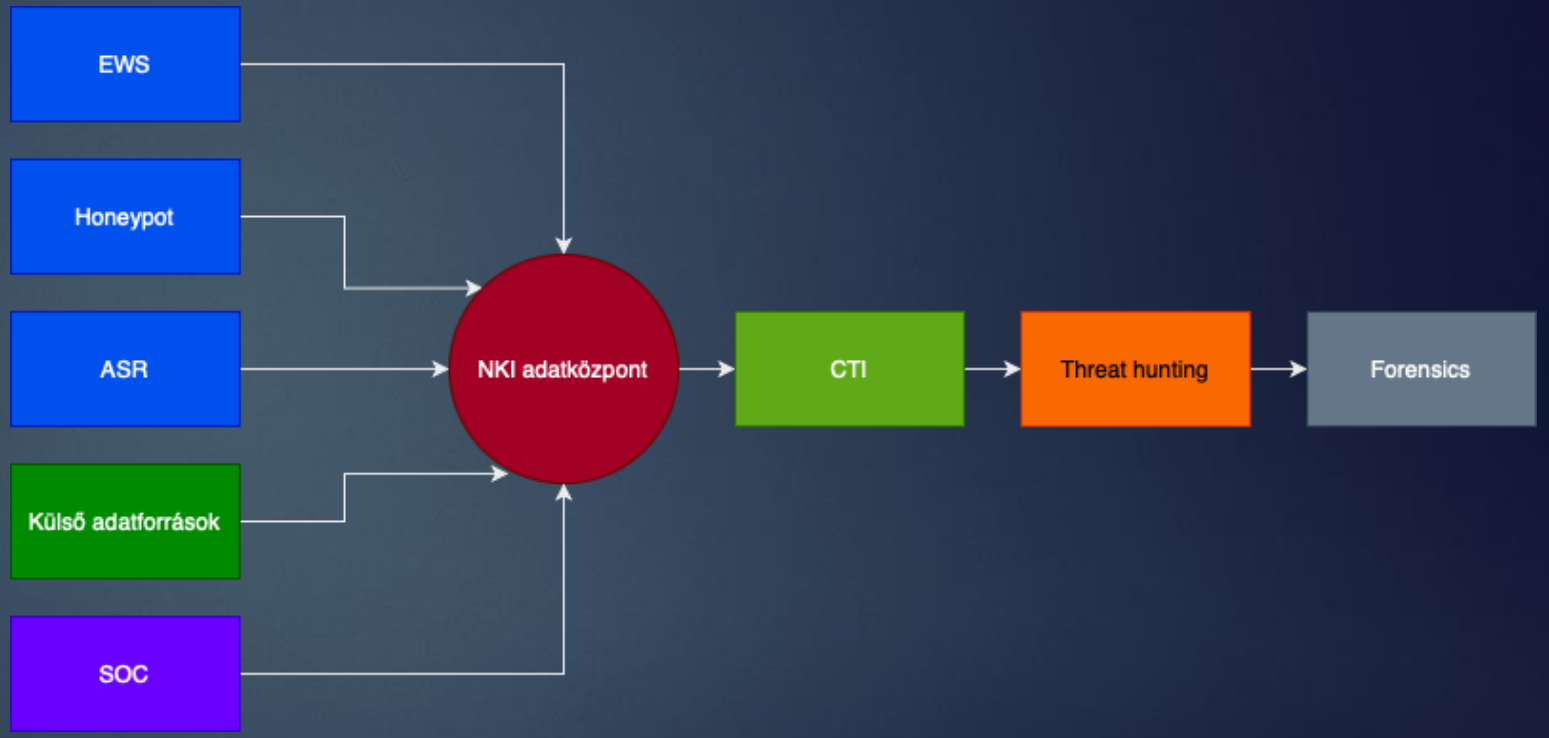
Cyber Threat Intelligence

Threat hunting

Forensic és IH

Tehát

- SOC-ol a CSIRT?
- Igen és nem!



- Adatot gyűjt és felhasználja
- Szolgáltatásként SOC építőelemeket nyújt ügyfeleinek

Kibertámadás!

Köszönöm a figyelmet!