NEMZETI
KÖZSZOLGÁLATI
EGYETEM
A HAZA SZOLGÁLATÁBAN

Egy Kiberbiztonsági Műveleti Központ (CSOC) megtervezése

Gyebnár Gergő

Nemzeti Közszolgálati Egyetem

Konzulens: Dr. Krasznay Csaba

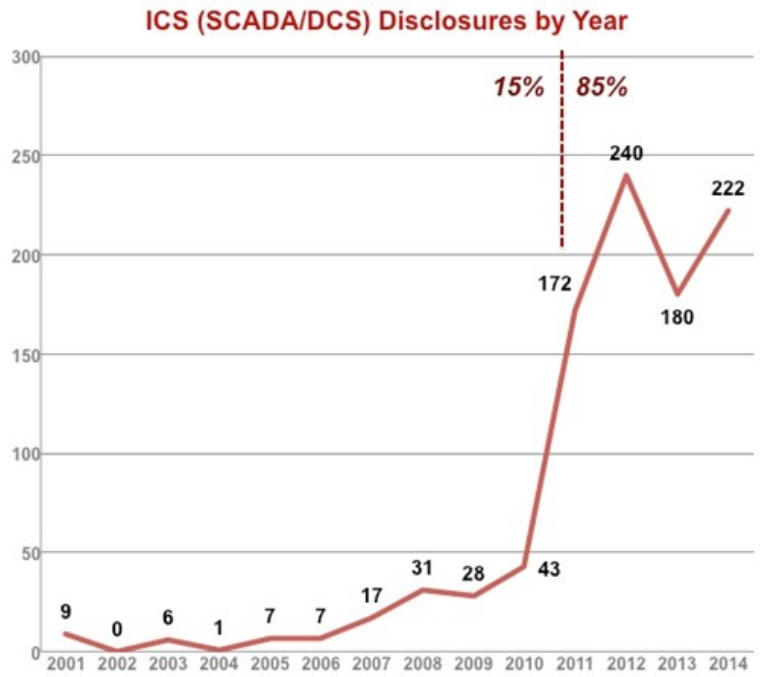
NEMZETI
KÖZSZOLGÁLATI
EGYETEM
A HAZA SZOLGÁLATÁBAN

A dolgozat felépítése

- Bevezető; kritikus infrastruktúrák biztonsága; fenyegetések
- CSOC; SIEM rendszer
- OSSIM
- Üzemeltetés

NEMZETI KÖZSZOLGÁLATI EGYETEM
A HAZA SZOLGÁLATÁBAN

ICS sérülékenységek



NEMZETI KÖZSZOLGÁLATI EGYETEM
A HAZA SZOLGÁLATÁBAN

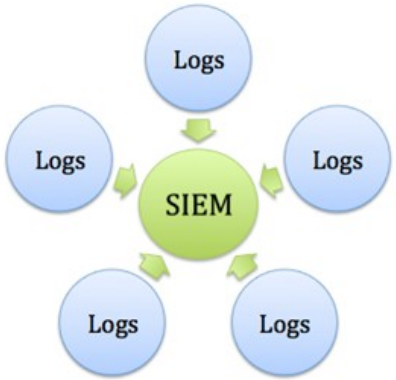
CSOC – SIEM?

- Hol? Ki? Minek?
- EOC, TOC, NOC
- Cél = komplex, specifikus incidens kezelő platform létrehozása
- Szempontok = teljeskörű személyre szabhatóság, „hardenelhetőség”

NEMZETI KÖZSZOLGÁLATI EGYETEM
A HAZA SZOLGÁLATÁBAN

OSSIM

- **Mi ez?**
- **Nyílt forráskód**
- **Integrálhatóság**
- **Fejleszthetőség**
- **Modularitás**



- Biztonsági információk kezelése
- Biztonsági események kezelése
- Eszközök felderítése és kezelése
- Log menedzsment
- IDS (behatolás azonosítás)
- HIDS (kliens oldali behatolás azonosítás)

- Sérülékenységi vizsgáló
- Forgalomelemzés
- Hoszt,- és szolgáltatásrendelkezésre állásfigyelés
- Netflow elemzés
- Incidens menedzsment
- Jelentéskészítés

NEMZETI
KÖZSZOLGÁLATI
EGYETEM
A HAZA SZOLGÁLATÁBAN

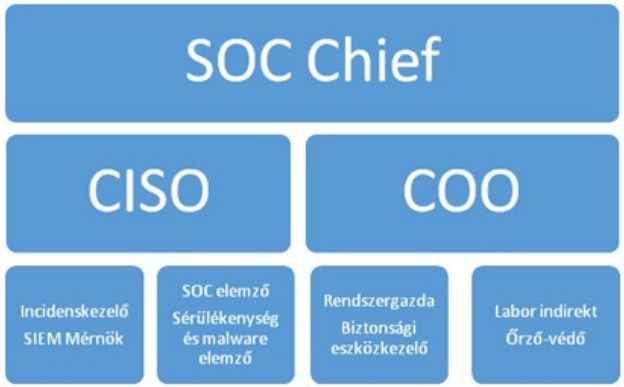
Opciós funkciók

- Sploitware
- Honeypot - DCEPT; MHN Modern Honey Network
- Razorback
- EMET
- ZABBIX; Sensu
- Securityonion

NEMZETI KÖZSZOLGÁLATI EGYETEM
A HAZA SZOLGÁLATÁBAN

Üzemeltetés

- Személyzeti struktúra - CSIRT development
- Képzés
- Objektum
- Költségvetés



NEMZETI KÖZSZOLGÁLATI EGYETEM
A HAZA SZOLGÁLATÁBAN

Összegzés

- A jövő katonai erődje
- Humán erőforrás optimalizálás

Nem csupán a „biztonságos”, sokkal inkább védhető IT a cél.

NEMZETI
KÖZSZOLGÁLATI
EGYETEM
A HAZA SZOLGÁLATÁBAN

Köszönöm a figyelmet!

Gyebnár Gergő