Az adatözönön túl – CTI egy SOC-ban

2024.05.02

SZABÓ GÁBOR

Cyber Security Advisor, EURO ONE

Motiváció

A “mi esetünk tanulmánya”

- Rendszerezési elv
- Gyakorlati alkalmazás, folyamatok illesztési pontjainak bemutatása

Kiindulás

FIRST definíciója:

“A CTI olyan információk szisztematikus gyűjtése, elemzése és megosztása, amelyek egy szervezet kibertérben, illetve bizonyos mértékig a fizikai térben történő működésére vonatkoznak.

Célja, hogy minden döntéshozói szinten tájékoztatásul szolgáljon.

Az elemzés az aktuális és a jövőbeni fenyegetésekről egy valós helyzetismeret kialakítását támogatja.”

Kiindulás

FIRST definíciója:

“A CTI olyan információk szisztematikus gyűjtése, elemzése és megosztása, amelyek egy szervezet kibertérben, illetve bizonyos mértékig a fizikai térben történő működésére vonatkoznak.

Célja, hogy minden döntéshozói szinten tájékoztatásul szolgáljon.

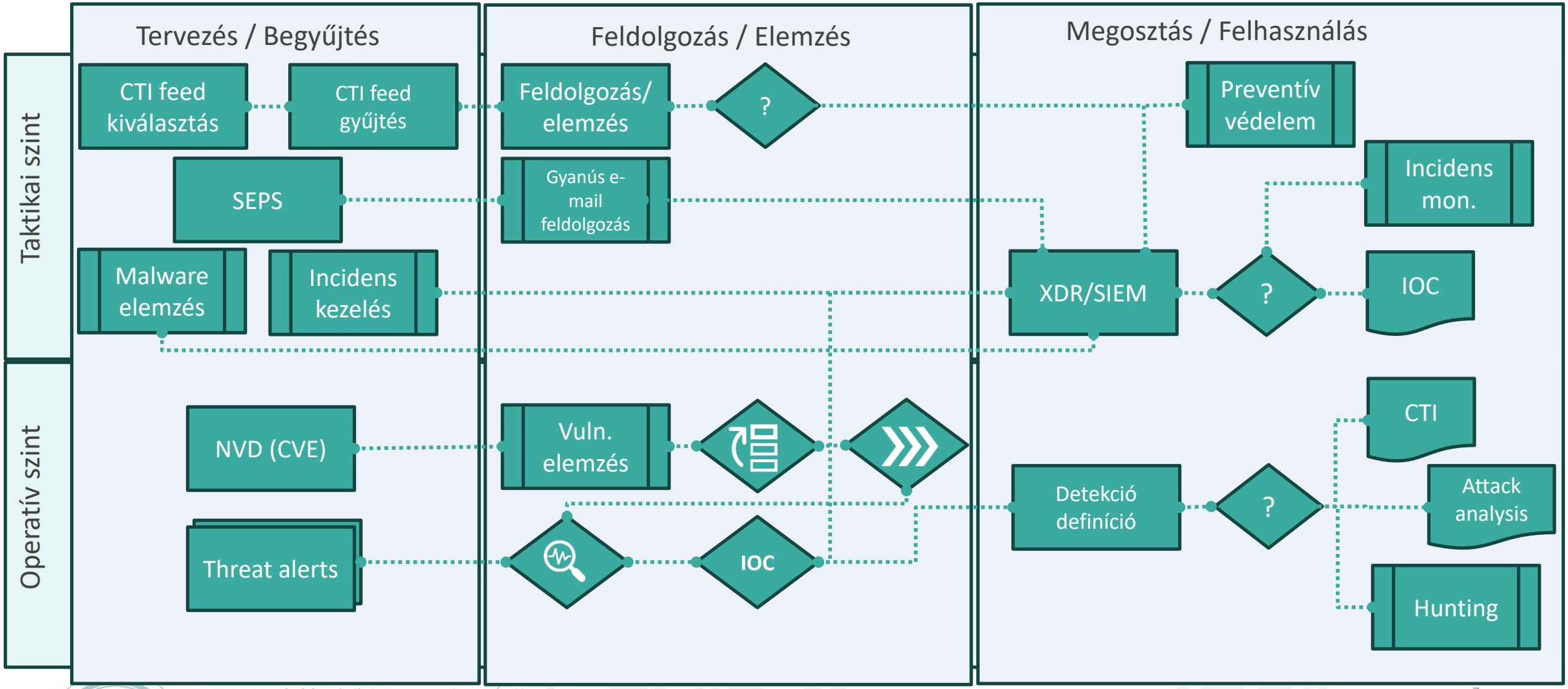
Az elemzés az aktuális és a jövőbeni fenyegetésekről egy valós helyzetismeret kialakítását támogatja.”

“Szisztematikus”

“Szintek”

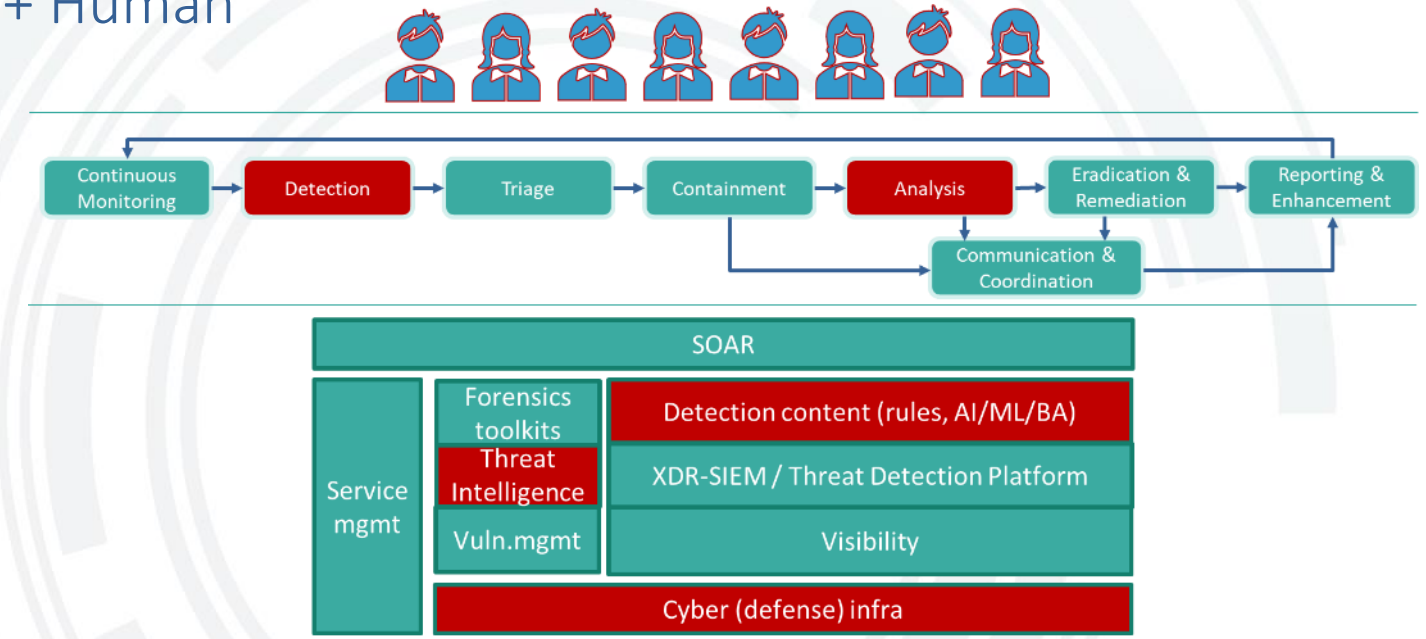
01	Stratégiai	magasszintű információ, statégiai felelősök részére
02	Operatív	napi üzletmenetre relevanciával bíró információ, operatív vezetők részére
03	Taktikai / Technikai	adott támadó által használt TTP-kről (Tools, Tactics, and Techniques) információ, elemzők részére

SOC folyamatok illesztése



CTI és a SOC

- CTI a SOC-ban: detekciós tartalom készítéséhez ad alapot
- CTI ≠ IOC
- CTI = Technológia + Folyamat + Humán
- Házon belül is „bányászható”



Köszönöm!

euroone