Lehet CTI-ozni inteventory nélkül?

Marsi Tamás
Nemzetbiztonsági Szakszolgálat
Nemzeti Kibervédelmi Intézet

EIVOK-47

Mégis, lehet?


NO, SIR!
ABSOLUTELY NOT!
yam.co


WE'RE TRYING, WE'RE TRYING!


INVENTORY MANAGER
"I THINK WE HAVE ENOUGH INVENTORY"
makeameme.org

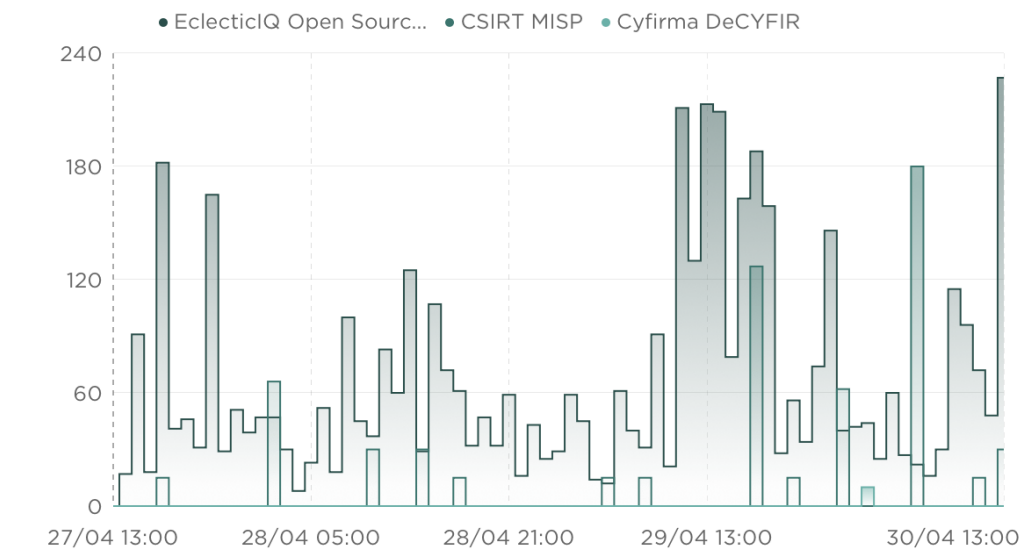
Jó, van egy csomó értelmetlen adatom! És?

Mi tud történni az adatokkal?

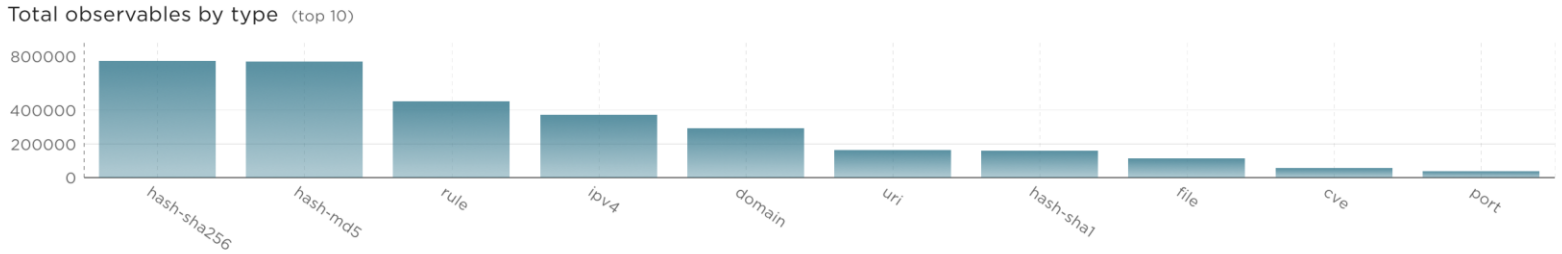
5 879 928 ↑ 13 928 (last 72h)
TOTAL ENTITIES AND OBSERVABLES

2 785 851 ↑ 5 494 (last 72h)
TOTAL ENTITIES

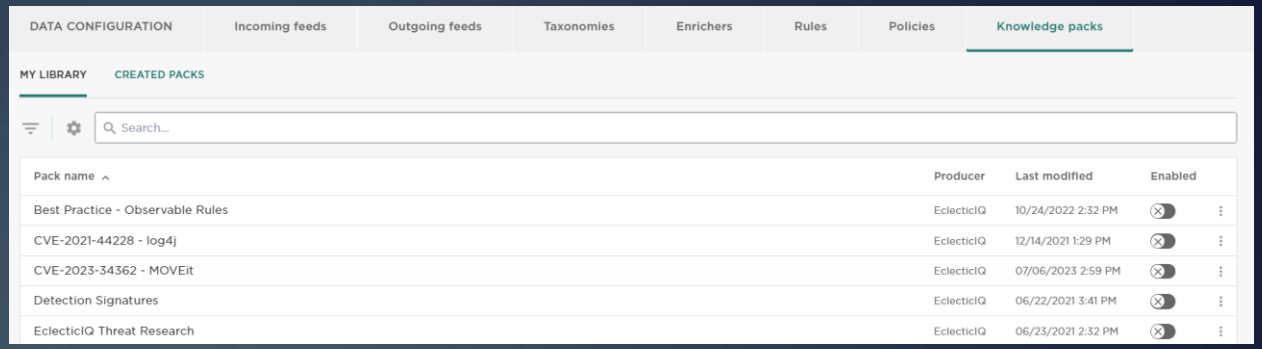
3 094 077 ↑ 8 434 (last 72h)
TOTAL OBSERVABLES

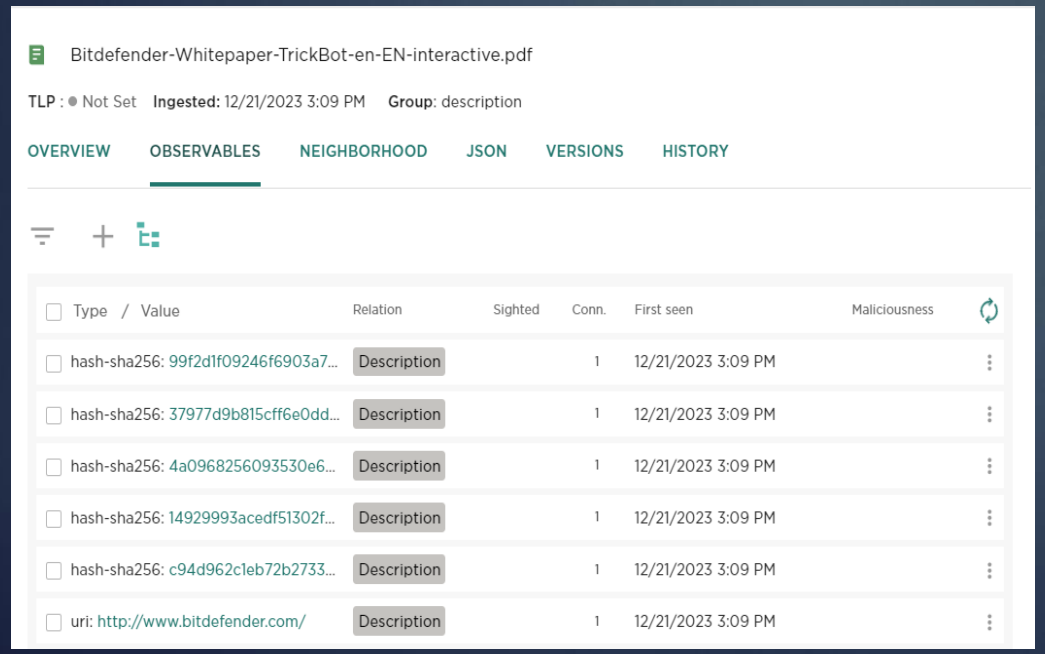


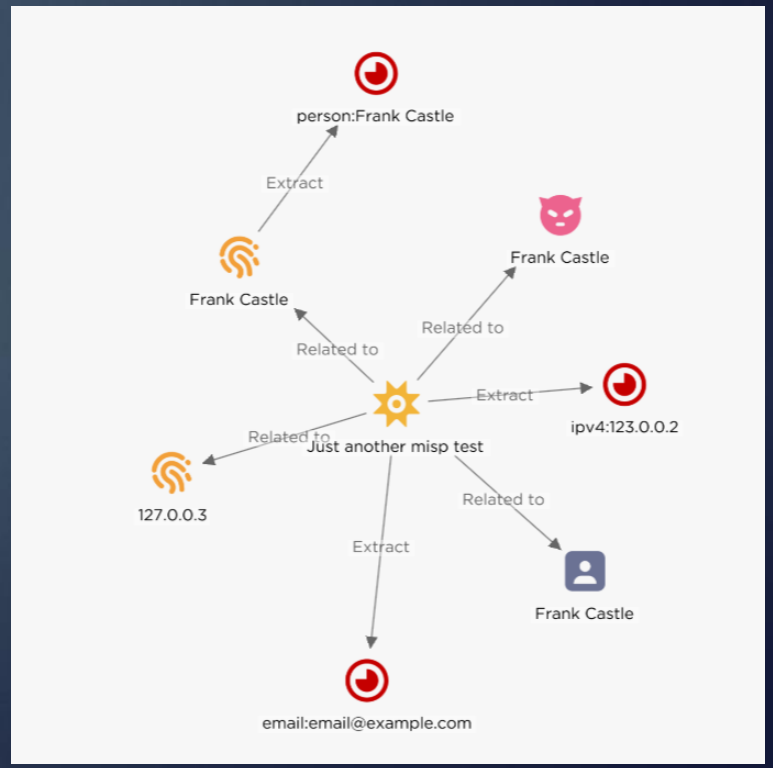
pl. meg lehet számolni!



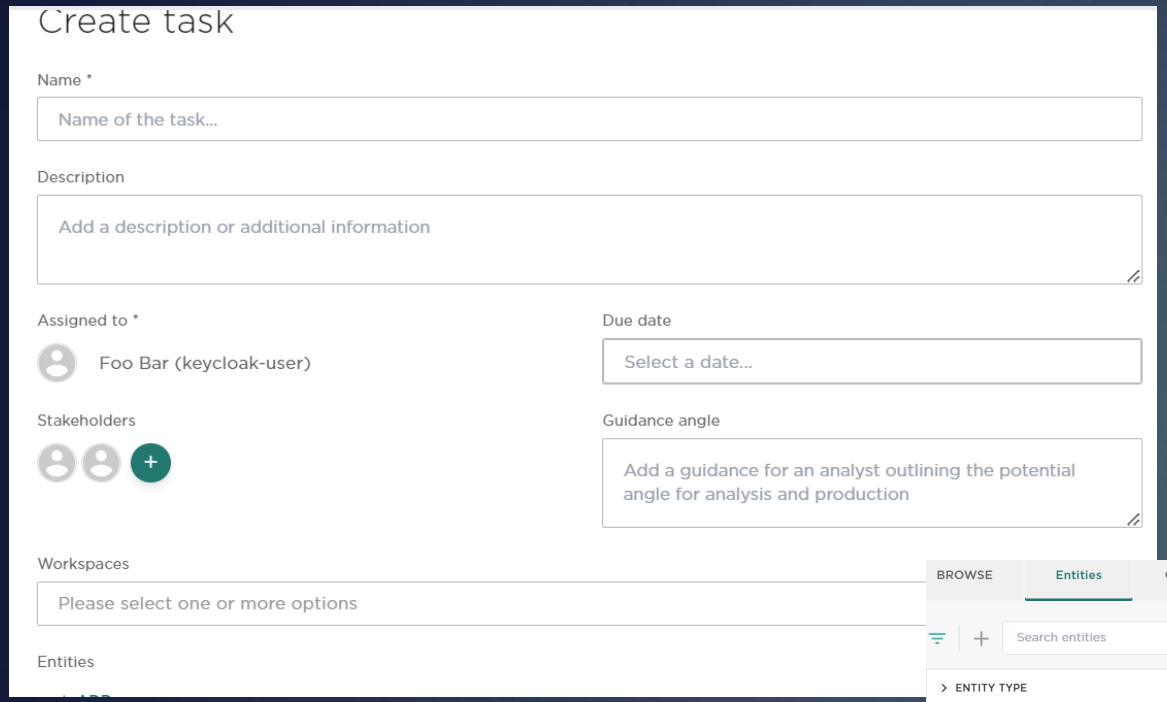
Elemzés és vizualizáció

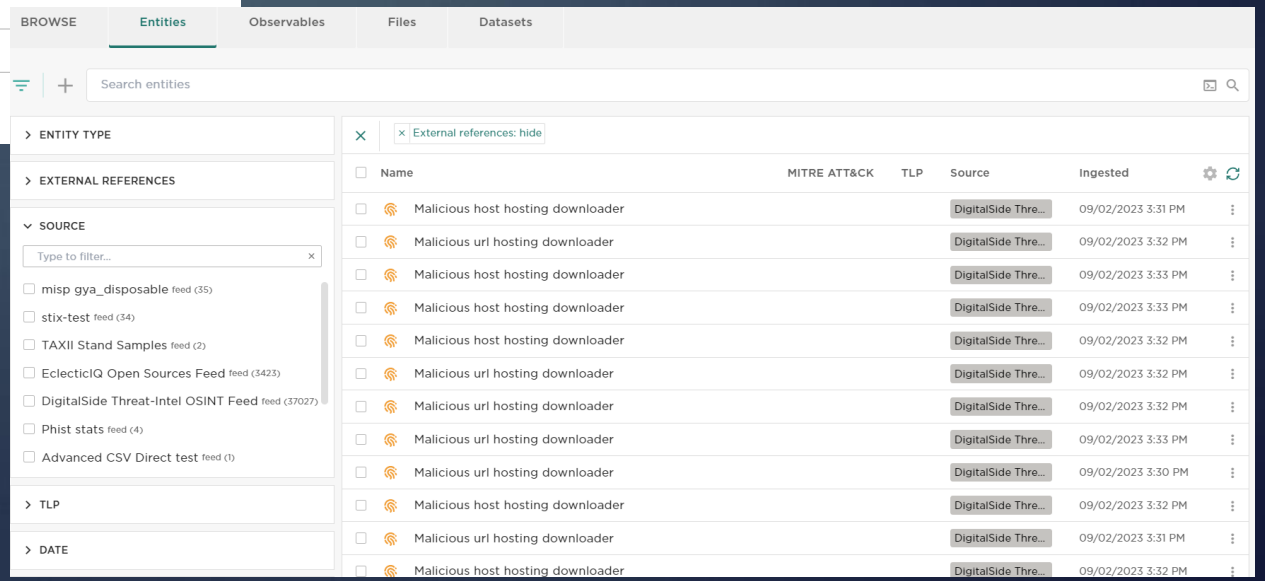




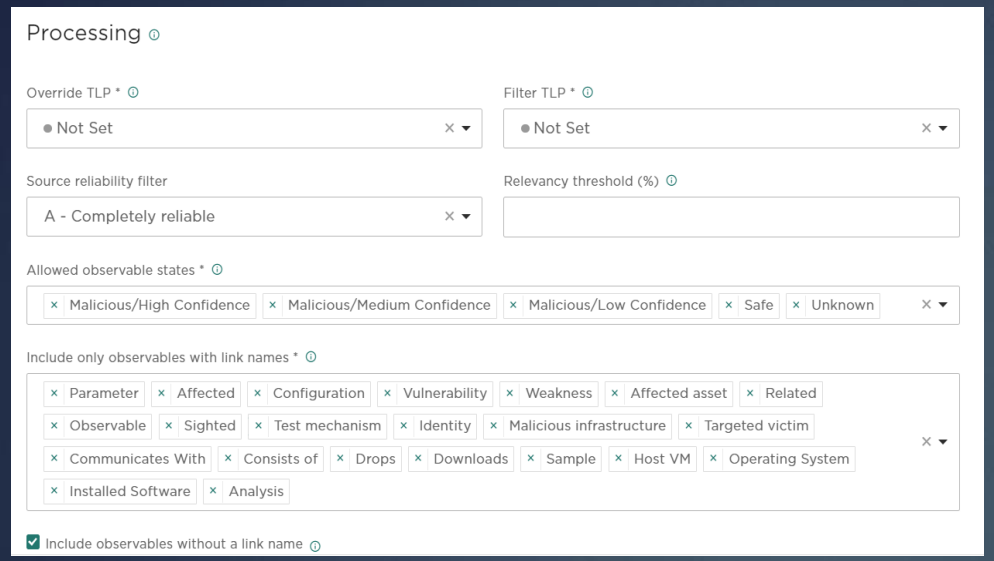


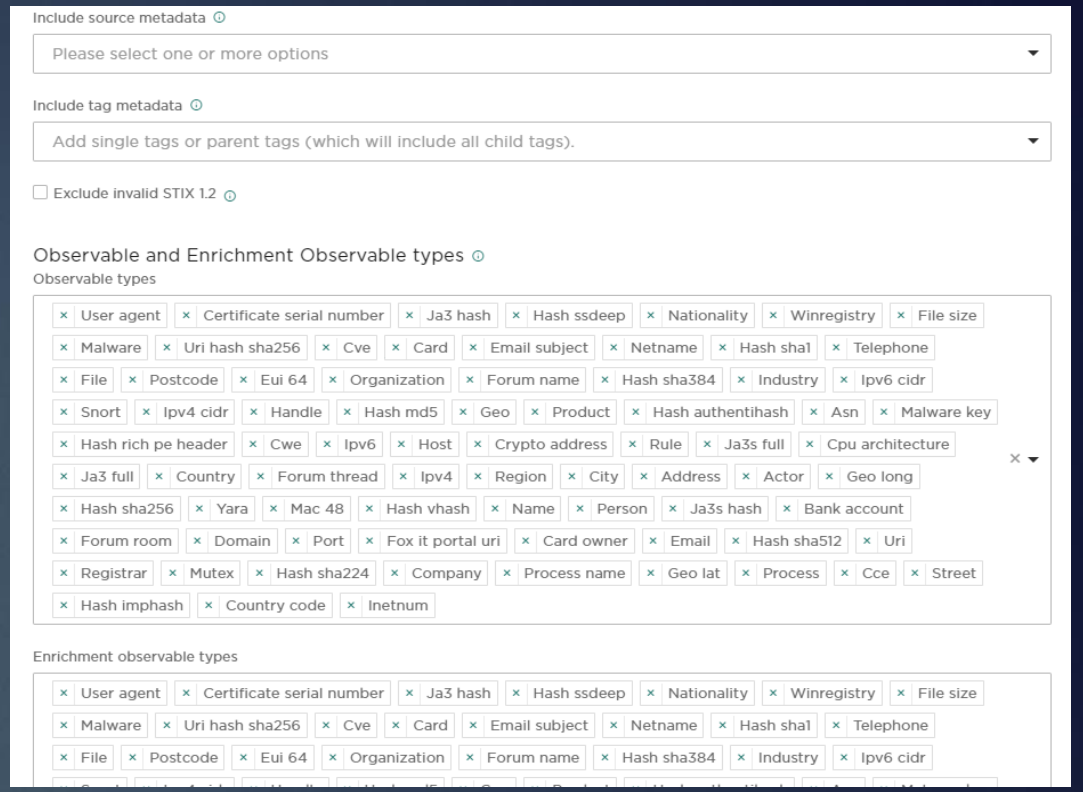
Tasking és searching





Disszemináció és adatdúsítás



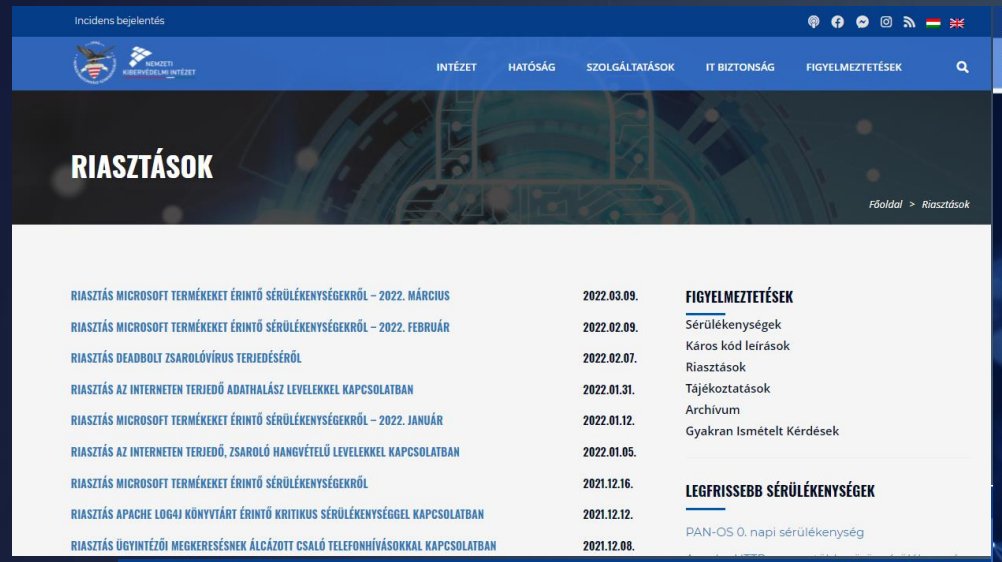


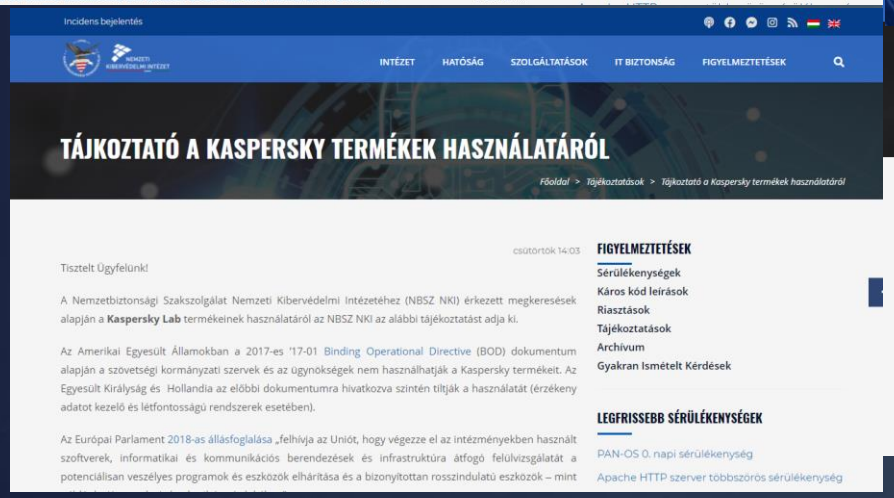
Tervezett eredménytermékek

Szektorspecifikus jelentések	Ajánlások	Pontosabb riasztások
Stratégiai támogatás	Célzott awareness tevékenység	Feed, szabályok


Adatok
Feedek
Incidensek
EWS
Honeypot
Elemzés
Trend
Korreláció
Összehasonlítás
Termékek
Célzott elemzések
Általános információk
Trendelemzések

Hol tájékozódjak?





Köszönöm a figyelmet!

tamas.marsi@nki.gov.hu

Kibertámadás! podcast

LinkedIn

nki.gov.hu