

Lehet CTI-ozni inteventory nélkül?

Marsi Tamás

Nemzetbiztonsági Szakszolgálat
Nemzeti Kibervédelmi Intézet

EIVOK-47



Mégis, lehet?



NO, SIR!

ABSOLUTELY NOT!

yoml.co





INVENTORY MANAGER

**"I THINK WE HAVE ENOUGH
INVENTORY"**

makeameme.org



Jó, van egy csomó értelmetlen adatom!
És?

Csak tudnám,
mit jelentenek
ezek a...



COUB
by @punkpapa



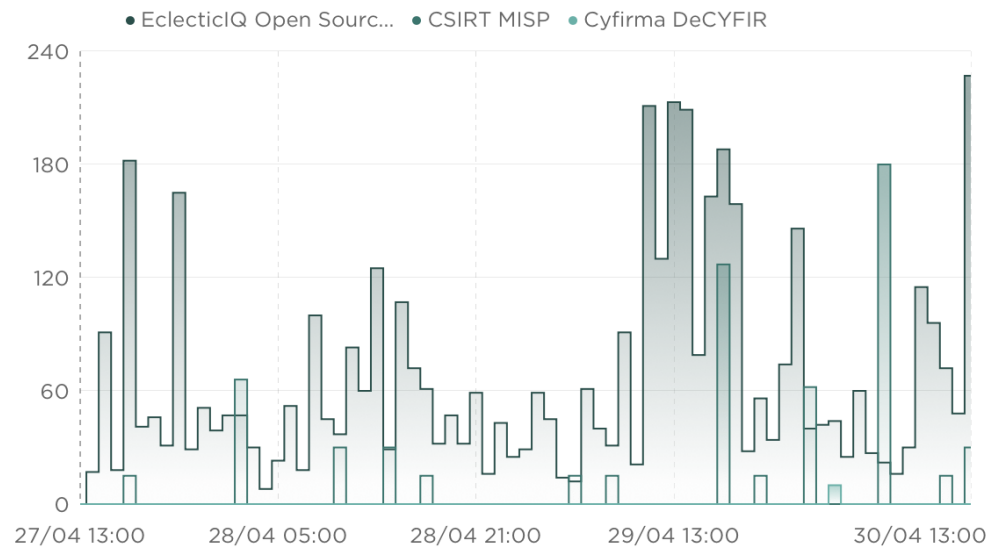
Mi tud történni az adatokkal?

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

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

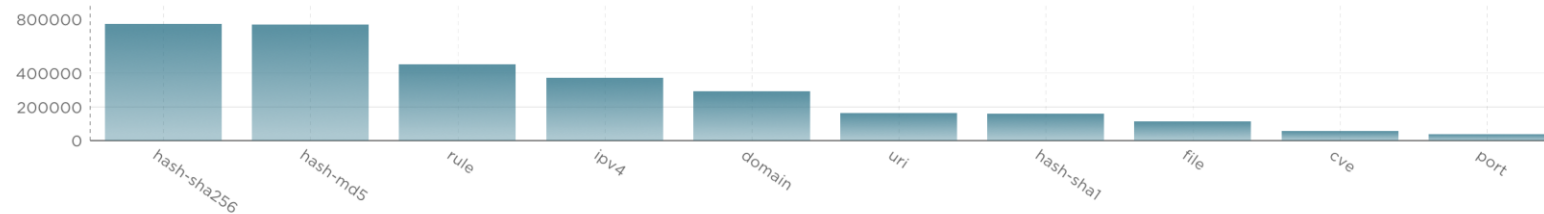
3 094 077 ↑ 8 434 (last 72h)
TOTAL OBSERVABLES

Ingested entities by feed (72h)



pl. meg lehet számolni!

Total observables by type (top 10)





Elemzés és vizualizáció

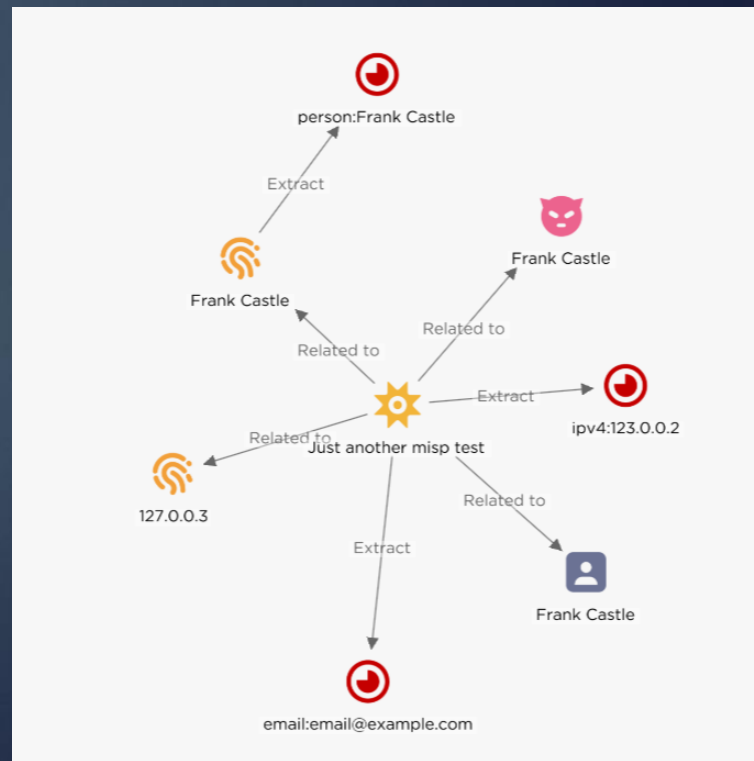
DATA CONFIGURATION	Incoming feeds	Outgoing feeds	Taxonomies	Enrichers	Rules	Policies	Knowledge packs
MY LIBRARY CREATED PACKS							
Q Search...							
Pack name ^	Producer	Last modified	Enabled				
Best Practice - Observable Rules	EclectIQ	10/24/2022 2:32 PM	<input type="checkbox"/>				
CVE-2021-44228 - log4j	EclectIQ	12/14/2021 1:29 PM	<input type="checkbox"/>				
CVE-2023-34362 - MOVEit	EclectIQ	07/06/2023 2:59 PM	<input type="checkbox"/>				
Detection Signatures	EclectIQ	06/22/2021 3:41 PM	<input type="checkbox"/>				
EclectIQ Threat Research	EclectIQ	06/23/2021 2:32 PM	<input type="checkbox"/>				

Bitdefender-Whitepaper-TrickBot-en-EN-interactive.pdf

TLP: Not Set Ingested: 12/21/2023 3:09 PM Group: description

OVERVIEW OBSERVABLES NEIGHBORHOOD JSON VERSIONS HISTORY

Type / Value	Relation	Sighted	Conn.	First seen	Maliciousness
hash-sha256: 99f2d1f09246f6903a7...	Description	1		12/21/2023 3:09 PM	
hash-sha256: 37977d9b815cff6e0dd...	Description	1		12/21/2023 3:09 PM	
hash-sha256: 4a0968256093530e6...	Description	1		12/21/2023 3:09 PM	
hash-sha256: 14929993acedf51302f...	Description	1		12/21/2023 3:09 PM	
hash-sha256: c94d962c1eb72b2733...	Description	1		12/21/2023 3:09 PM	
uri: http://www.bitdefender.com/	Description	1		12/21/2023 3:09 PM	





Disszemináció és adatdúsítás

Processing

Override TLP * Filter TLP *

Source reliability filter Relevancy threshold (%)

Allowed observable states *

Include only observables with link names *

Include observables without a link name

Include source metadata

Include tag metadata

Exclude invalid STIX 1.2

Observable and Enrichment Observable types

Observable types

- User agent, Certificate serial number, Ja3 hash, Hash ssdeep, Nationality, Winregistry, File size, Malware, Uri hash sha256, Cve, Card, Email subject, Netname, Hash sha1, Telephone, File, Postcode, Eui 64, Organization, Forum name, Hash sha384, Industry, Ipv6 cidr, Snort, Ipv4 cidr, Handle, Hash md5, Geo, Product, Hash authentihash, Asn, Malware key, Hash rich pe header, Cwe, Ipv6, Host, Crypto address, Rule, Ja3s full, Cpu architecture, Ja3 full, Country, Forum thread, Ipv4, Region, City, Address, Actor, Geo long, Hash sha256, Yara, Mac 48, Hash vhash, Name, Person, Ja3s hash, Bank account, Forum room, Domain, Port, Fox it portal uri, Card owner, Email, Hash sha512, Uri, Registrar, Mutex, Hash sha224, Company, Process name, Geo lat, Process, Cce, Street, Hash impash, Country code, Inetnum

Enrichment observable types

- User agent, Certificate serial number, Ja3 hash, Hash ssdeep, Nationality, Winregistry, File size, Malware, Uri hash sha256, Cve, Card, Email subject, Netname, Hash sha1, Telephone, File, Postcode, Eui 64, Organization, Forum name, Hash sha384, Industry, Ipv6 cidr

Observable	Source	Count	Timestamp	Status
ip4: 184.168.192.168	Observable +3	1	08/22/2023 1:54 PM	
city: Centreville	RIPEstat Whois		08/08/2023 5:27 PM	
organization: American Registry...	RIPEstat Whois		08/08/2023 5:38 PM	
organization: GoDaddy.com, LL...	RIPEstat Whois		09/10/2023 11:17 PM	
city: Tempe	RIPEstat Whois		10/03/2023 8:40 AM	●
country: US	RIPEstat Whois		10/06/2023 6:07 AM	

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?



Incidens bejelentés

INTÉZET HATÓSÁG SZOLGÁLTATÁSOK IT BIZTONSÁG FIGYELMEZTETÉSEK

RIASZTÁSOK

Főoldal > Riasztások

RIASZTÁS MICROSOFT TERMÉKEKET ÉRINTŐ SÉRÜLÉKENYSÉGEKRŐL – 2022. MÁRCIUS	2022.03.09.	FIGYELMEZTETÉSEK
RIASZTÁS MICROSOFT TERMÉKEKET ÉRINTŐ SÉRÜLÉKENYSÉGEKRŐL – 2022. FEBRUÁR	2022.02.09.	Sérülékenységek
RIASZTÁS DEADBOLT ZSAROLÓVÍRUS TERJEDÉSÉRŐL	2022.02.07.	Káros kód leírások
RIASZTÁS AZ INTERNETEN TERJEDŐ ADATHALÁSZ LEVELEKKEL KAPCSOLATBAN	2022.01.31.	Riasztások
RIASZTÁS MICROSOFT TERMÉKEKET ÉRINTŐ SÉRÜLÉKENYSÉGEKRŐL – 2022. JANUÁR	2022.01.12.	Tájékoztatások
RIASZTÁS AZ INTERNETEN TERJEDŐ, ZSAROLÓ HANGVÉTELŐ LEVELEKKEL KAPCSOLATBAN	2022.01.05.	Archívum
RIASZTÁS MICROSOFT TERMÉKEKET ÉRINTŐ SÉRÜLÉKENYSÉGEKRŐL	2021.12.16.	Gyakran Ismételt Kérdések
RIASZTÁS APACHE LOGAI KÖNYVTÁRT ÉRINTŐ KRITIKUS SÉRÜLÉKENYSÉGGEL KAPCSOLATBAN	2021.12.12.	LEGFRISSEBB SÉRÜLÉKENYSÉGEK
RIASZTÁS ÜGYINTÉZŐI MEGKERESÉSNEK ÁLCÁZOTT CSALÓ TELEFONHÍVÁSOKKAL KAPCSOLATBAN	2021.12.08.	PAN-OS 0. napi sérülékenység

Incidens bejelentés **Frisse NKI riasztás jelent meg**

INTÉZET HATÓSÁG HÍREK TUDÁSKÖZPONT FIGYELMEZTETÉSEK

Kiemelt témák

Jelszavak **Kéretlen levelek** **Zsárolóvírus** **Adathalászat**

Hogyan cselezhetjük ki a QR-kódos csalókat?

Incidens bejelentés

INTÉZET HATÓSÁG SZOLGÁLTATÁSOK IT BIZTONSÁG FIGYELMEZTETÉSEK

TÁJKOZTATÓ A KASPERSKY TERMÉKEK HASZNÁLATÁRÓL

Főoldal > Tájékoztatások > Tájékoztató a Kaspersky termékek használatáról

Tisztelt Ügyfelünk!

2023.01.03.

FIGYELMEZTETÉSEK

Sérülékenységek

Káros kód leírások

Riasztások

Tájékoztatások

Archívum

Gyakran Ismételt Kérdések

LEGFRISSEBB SÉRÜLÉKENYSÉGEK

PAN-OS 0. napi sérülékenység

Apache HTTP szerver többszörös sérülékenység

KÁROS KÓD LEÍRÁSOK

Főoldal > Káros kód leírások

HERMETICWIPER LEÍRÁS	2022.02.25.	MAGAS	FIGYELMEZTETÉSEK
EGREGOR RANSOMWARE LEÍRÁS	2020.11.02.	KÖZEPES	Sérülékenységek
SHELLBOT KÁROS KÓD LEÍRÁS	2020.11.02.	KÖZEPES	Káros kód leírások
TYCOON RANSOMWARE LEÍRÁS	2020.09.02.	KÖZEPES	Riasztások
WASTEDLOCKER RANSOMWARE KÁROS KÓD LEÍRÁS	2020.08.18.	KÖZEPES	Tájékoztatások
NETWALKER RANSOMWARE	2020.07.06.	KÖZEPES	Archívum
KILLMBR.CORN_A	2020.04.07.	KÖZEPES	Gyakran Ismételt Kérdések
COVIDLOCK ZSAROLÓVÍRUS	2020.03.19.	KÖZEPES	LEGFRISSEBB SÉRÜLÉKENYSÉGEK

Köszönöm a figyelmet!

tamas.marsi@nki.gov.hu



Kibertámadás!
podcast



LinkedIn



nki.gov.hu

