Támadási gráfok alkalmazhatósága SOC-ban

Felhő szolgáltatási technológiák

Szöllősi Bence, Leposa Márkó,
Farkas Olivér, Pálinkás Zoltán,
Dargó Krisztián, Ujfalusi Zoltán,
Mészáros Ádám, Sámson
Norbert

Neumann János Informatikai Kar
Óbudai Egyetem
2022/23

Vörösné Dr. Bánáti-Baumann Anna
Dr. Fleiner Rita
Dr. Simon-Nagy Gabriella

Külső konzulens
Márton Márk Patrik

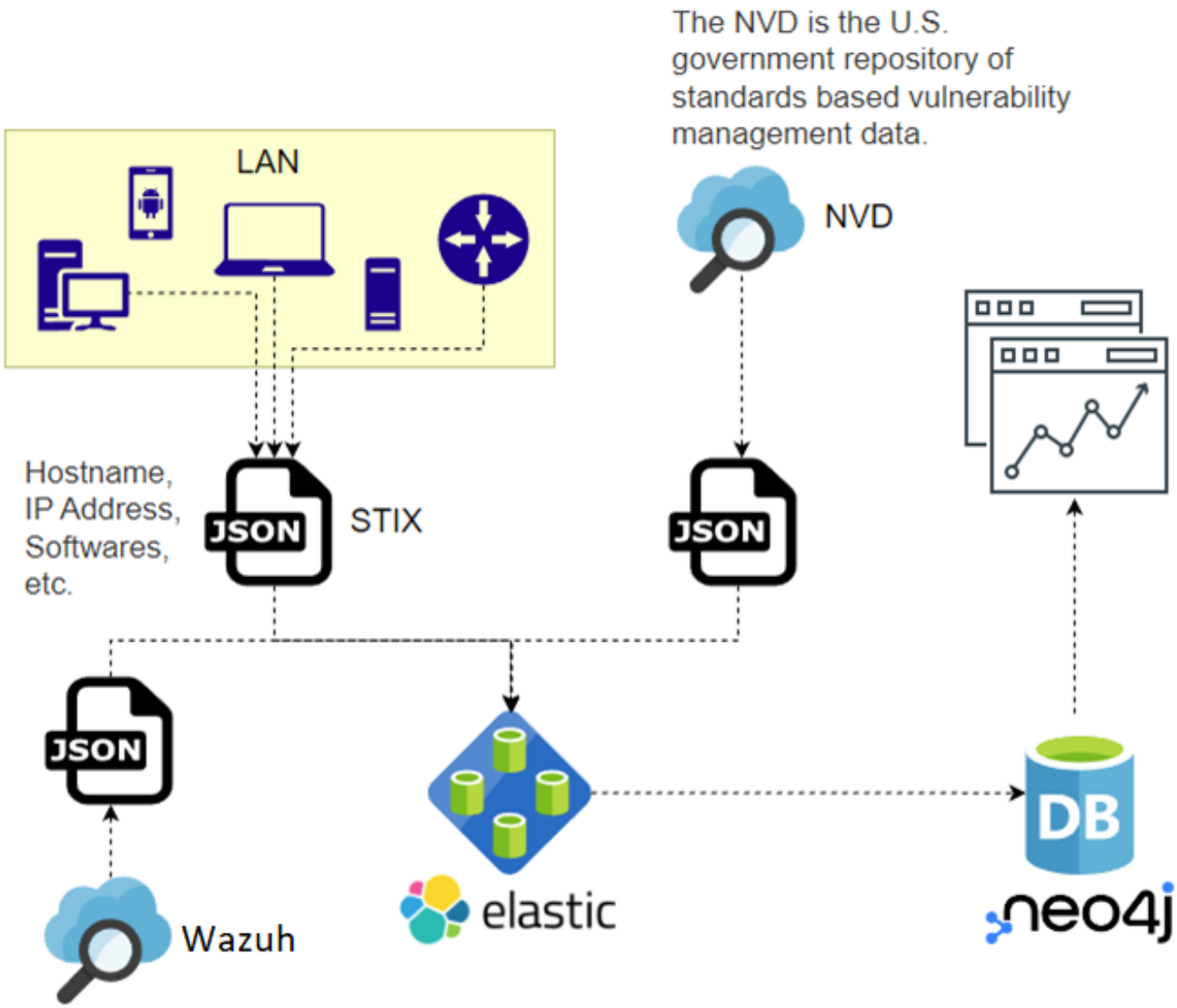
Attack Graph

- Sérülékenységek gyűjtése és elemzése
- Hálózat és infrastruktúra adatainak gyűjtése
- Támadási útvonalak szimulálása

Szerepük a projectben:

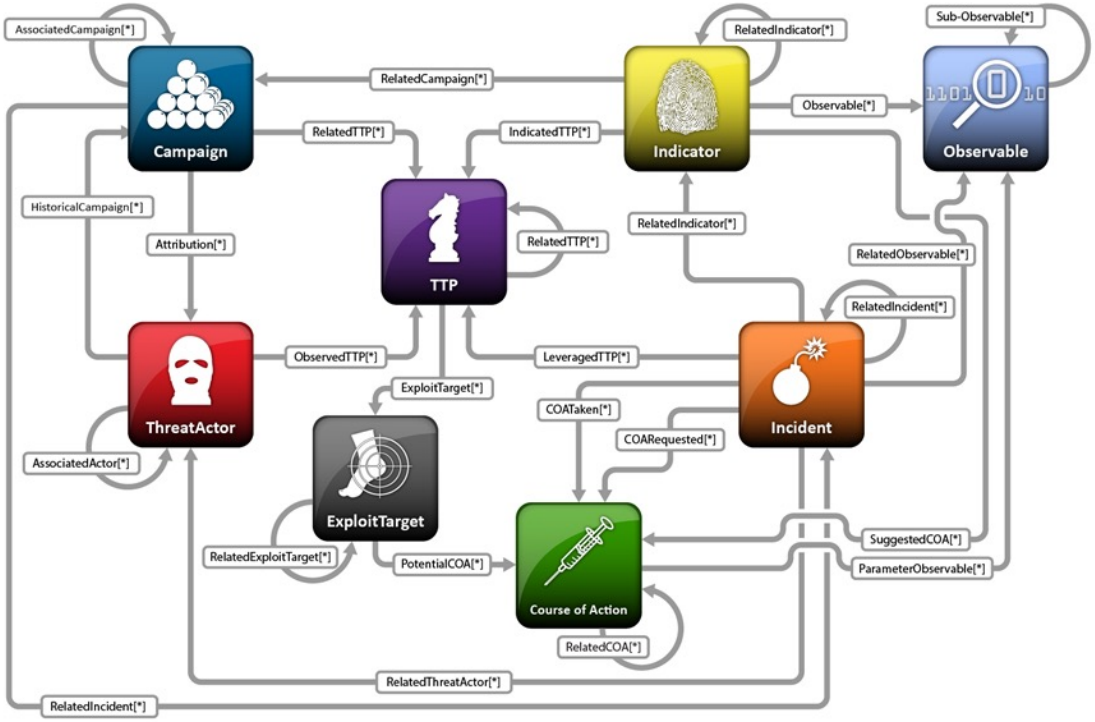
- A hálózati infrasturktúra sérülékenységeinek bemutatása
- Az sérülékenységek kategórizált megjelenítése / ábrázolása
- Támadások ábrázolása

Kiberbiztonsági elemző rendszer



Mi az a STIX?

- Structured Threat Information Expression
- Támadási információk megosztása
- Szabványosított adatmodellt definiál
  - STIX domain objects
  - STIX meta objects
  - STIX relationship objects
- Célja az egységesítés
  - Támadások elemzése
  - Támadási minták meghatározása
  - A támadásokra történő reakció kezelése (megelőzés, észlelés, válasz)



STIX domain and meta objects

attack-pattern, campaign, course-of-action, identity, indicator, malware, marking-definition, vulnerability

STIX relationship objects

indicates, mitigates, targets, uses

Examples:

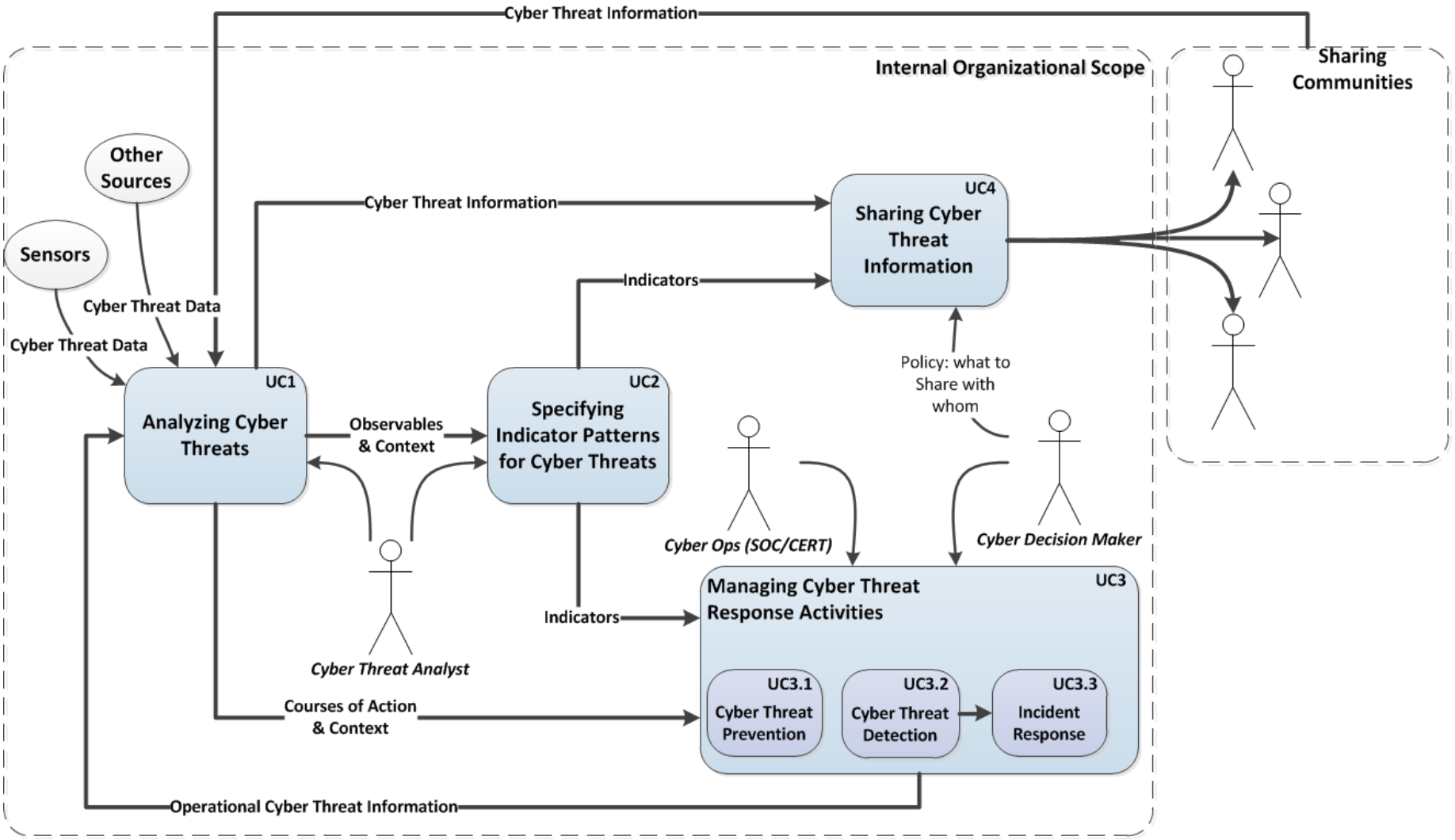
indicator SDO that can indicate a campaign or a malware
campaign using a malware or attack-pattern
campaign or attack-pattern targets a vulnerability

STIX példa: Threat Actor

Required Common Properties
type, spec_version, id, created, modified
Optional Common Properties
created_by_ref, revoked, labels, confidence, lang, external_references, object_marking_refs, granular_markings, extensions
Not Applicable Common Properties
defanged
Threat Actor Specific Properties
name, description, threat_actor_types, aliases, first_seen, last_seen, roles, goals, sophistication, resource_level, primary_motivation, secondary_motivations, personal_motivations

Property Name	Type	Description
type (required)	string	The value of this property **MUST** be threat-actor.
name (required)	string	A name used to identify this Threat Actor or Threat Actor group.
description (optional)	string	A description that provides more details and context about the Threat Actor, potentially including its purpose and its key characteristics.
threat_actor_types (optional)	list of type open-vocab	The type(s) of this threat actor. The values for this property **SHOULD** come from the threat-actor-type-ov open vocabulary.
aliases (optional)	list of type string	A list of other names that this Threat Actor is believed to use.
first_seen (optional)	timestamp	The time that this Threat Actor was first seen. This property is a summary property of data from sightings and other data that may or may not be available in STIX. If new sightings are received that are earlier than the first seen timestamp, the object may be updated to account for the new data.
last_seen (optional)	timestamp	The time that this Threat Actor was last seen. This property is a summary property of data from sightings and other data that may or may not be available in STIX. If new sightings are received that are later than the last seen timestamp, the object may be updated to account for the new data. If this property and the first_seen property are both defined, then this property **MUST** be greater than or equal to the timestamp in the first_seen property.
roles (optional)	list of type open-vocab	A list of roles the Threat Actor plays. The values for this property **SHOULD** come from the threat-actor-role-ov open vocabulary.
goals (optional)	list of type string	The high-level goals of this Threat Actor, namely, *what* are they trying to do. For example, they may be motivated by personal gain, but their goal is to steal credit card numbers. To do this, they may execute specific Campaigns that have detailed objectives like compromising point of sale systems at a large retailer.
sophistication (optional)	open-vocab	The skill, specific knowledge, special training, or expertise a Threat Actor must have to perform the attack. The value for this property **SHOULD** come from the threat-actor-sophistication-ov open vocabulary.
resource_level (optional)	open-vocab	The organizational level at which this Threat Actor typically works, which in turn determines the resources available to this Threat Actor for use in an attack. This attribute is linked to the sophistication property — a specific resource level implies that the Threat Actor has access to at least a specific sophistication level. The value for this property **SHOULD** come from the attack-resource-level-ov open vocabulary.
primary_motivation (optional)	open-vocab	The primary reason, motivation, or purpose behind this Threat Actor. The motivation is *why* the Threat Actor wishes to achieve the goal (what they are trying to achieve). For example, a Threat Actor with a goal to disrupt the finance sector in a country might be motivated by ideological hatred of capitalism. The value for this property **SHOULD** come from the attack-motivation-ov open vocabulary.

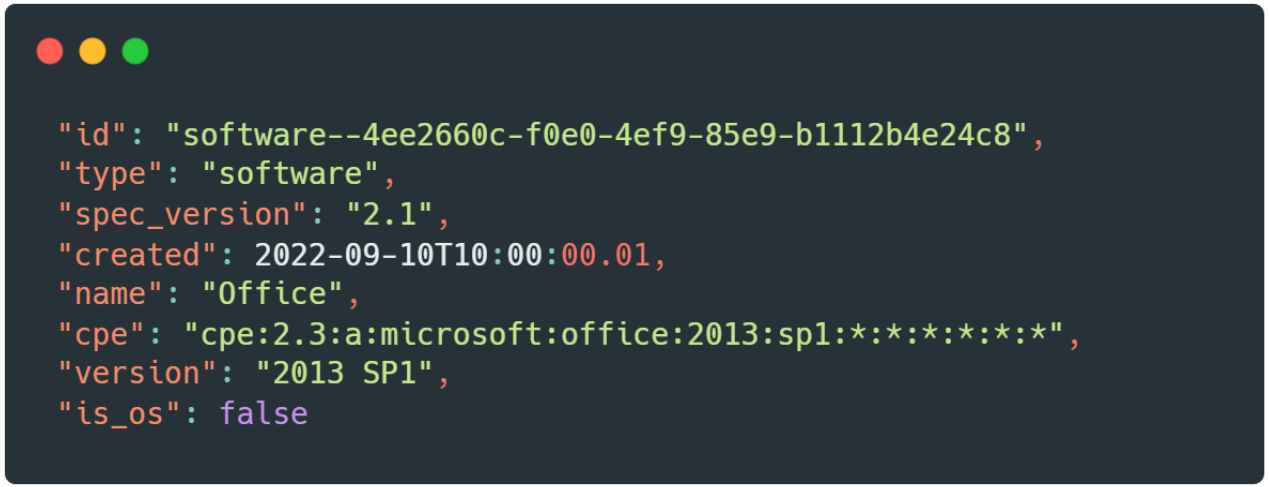
Mi az a STIX?


Cyber Threat Information
Internal Organizational Scope
Sharing Communities
Other Sources
Sensors
Cyber Threat Data
Cyber Threat Data
Cyber Threat Information
UC4
Sharing Cyber Threat Information
Indicators
Policy: what to Share with whom
UC1
Analyzing Cyber Threats
Observables & Context
UC2
Specifying Indicator Patterns for Cyber Threats
Cyber Ops (SOC/CERT)
Cyber Decision Maker
Cyber Threat Analyst
Indicators
Managing Cyber Threat Response Activities
UC3
UC3.1
Cyber Threat Prevention
UC3.2
Cyber Threat Detection
UC3.3
Incident Response
Courses of Action & Context
Operational Cyber Threat Information

Elasticsearch adatbázis

- Dokumentum tároló
- NoSQL adatbázis
- STIX formátumú adatok tárolása

Software Node



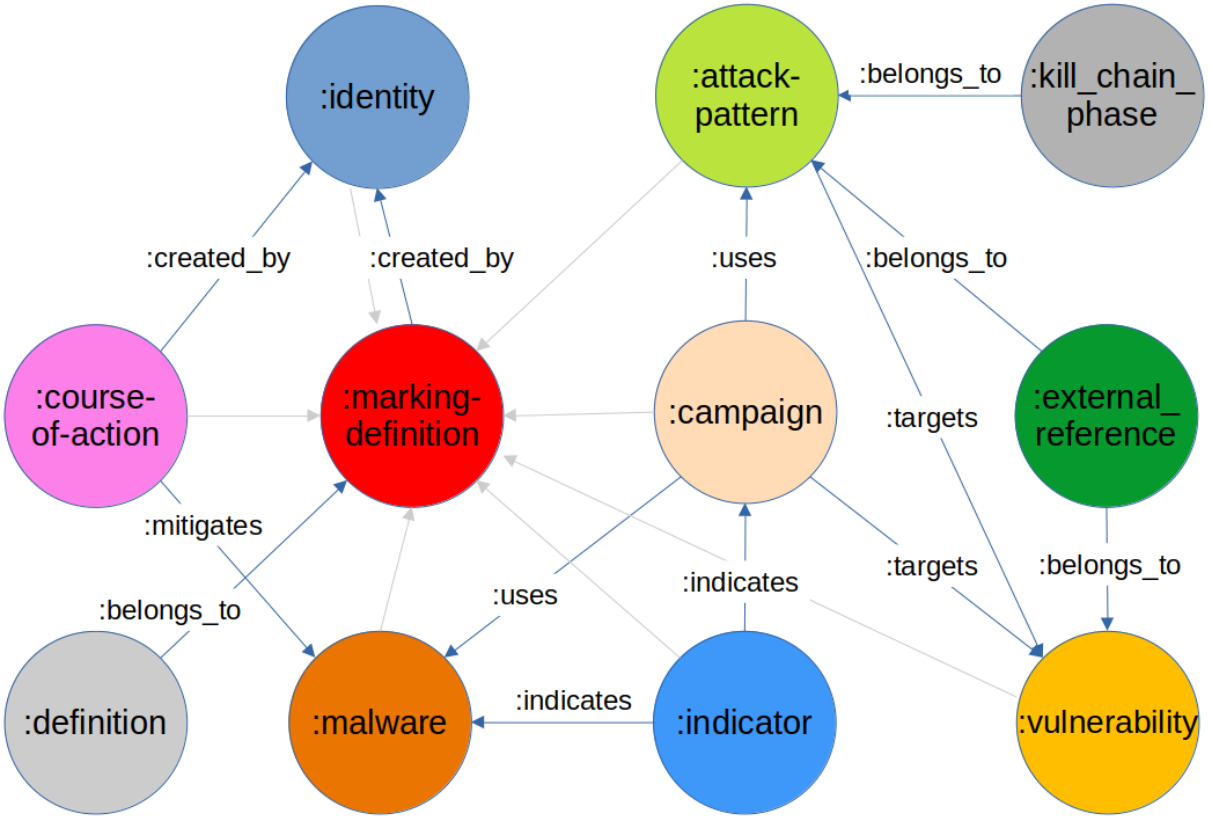
```
"id": "software--4ee2660c-f0e0-4ef9-85e9-b1112b4e24c8",
"type": "software",
"spec_version": "2.1",
"created": 2022-09-10T10:00:00.01,
"name": "Office",
"cpe": "cpe:2.3:a:microsoft:office:2013:sp1:*:*:*:*:*:*",
"version": "2013 SP1",
"is_os": false
```

Vulnerability Node

```
"id": "vulnerability--68ff5e6f-272b-48a2-b7bd-fe407fba8a4b",
"type": "vulnerability",
"spec_version": "2.1",
"created": 2022-09-10T10:00:00.01,
"name": "CVE-2022-29072",
"description": "** DISPUTED ** 7-Zip,
"external_references": []
```

Neo4j

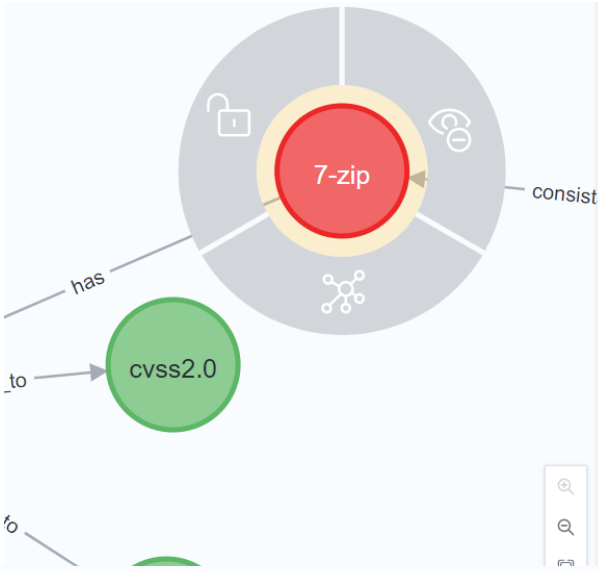
- Gráfok tárolása
- Az entitások közti kapcsolatokra fókuszál
- Cypher nyelv
- STIX megvalósítására alkalmas



Gráfadatbázis alkotóelemei

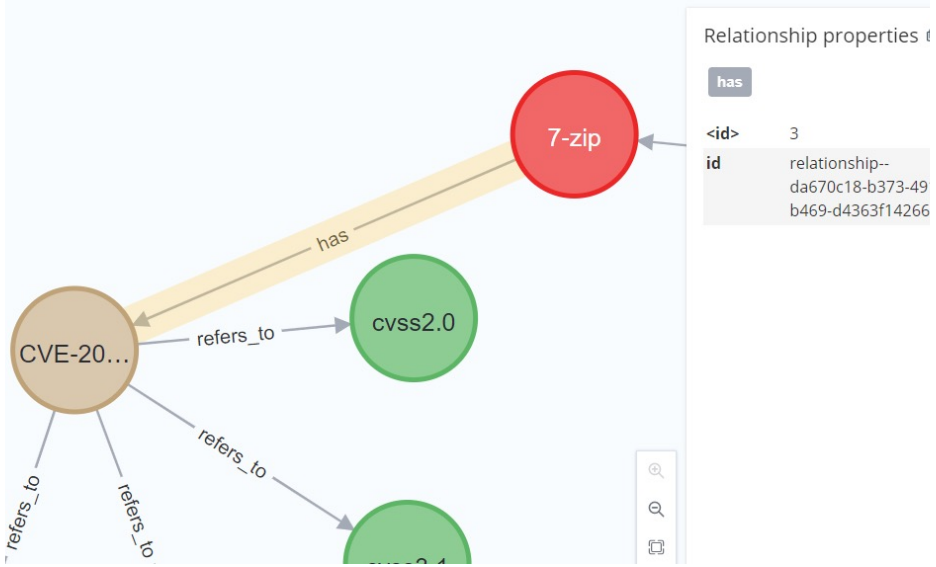
Csúcsok:

- Címkék
- Tulajdonságok
- Entitásokat reprezentál
- Kifinomult osztályhierarchia

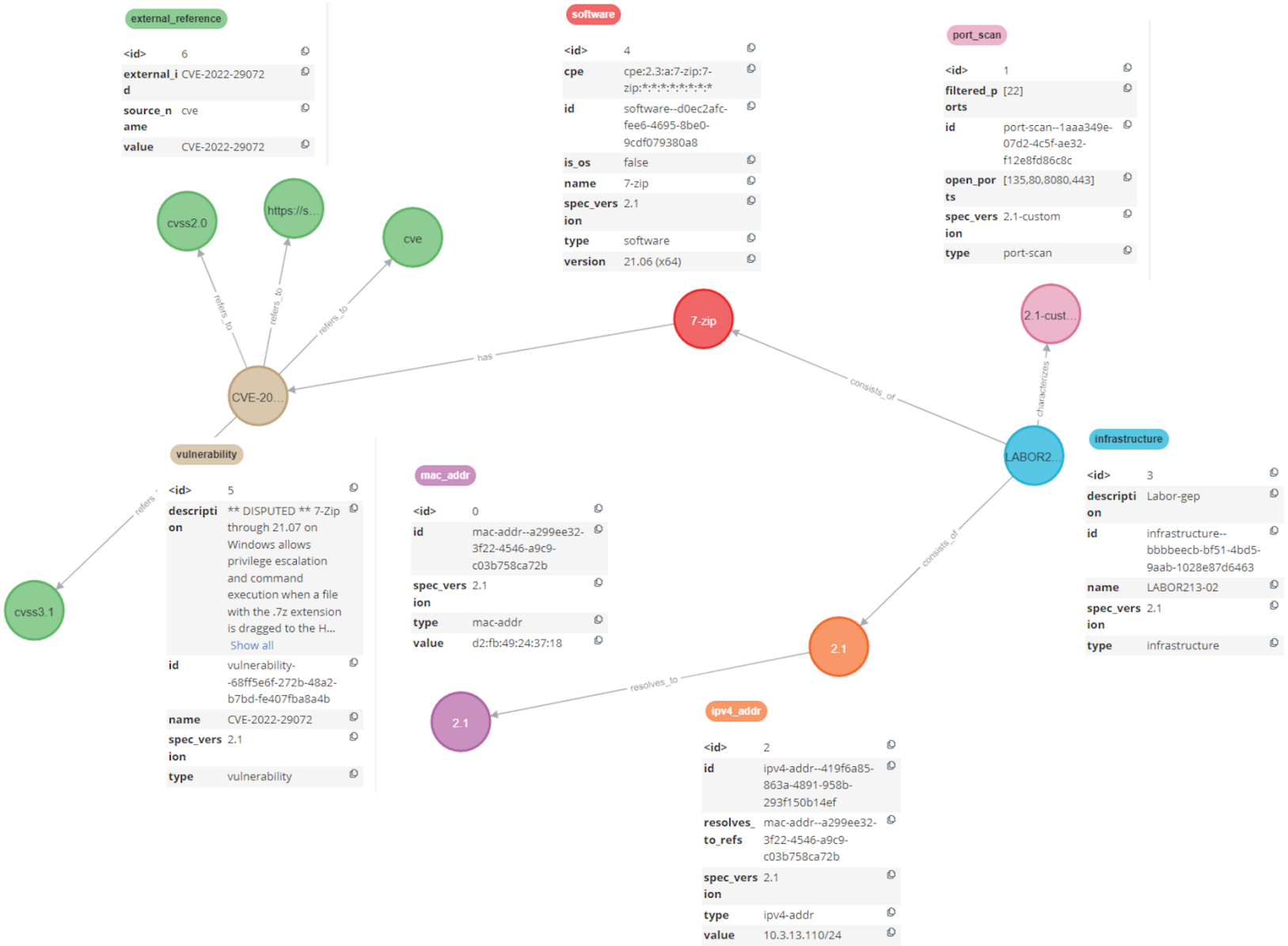


Élek:

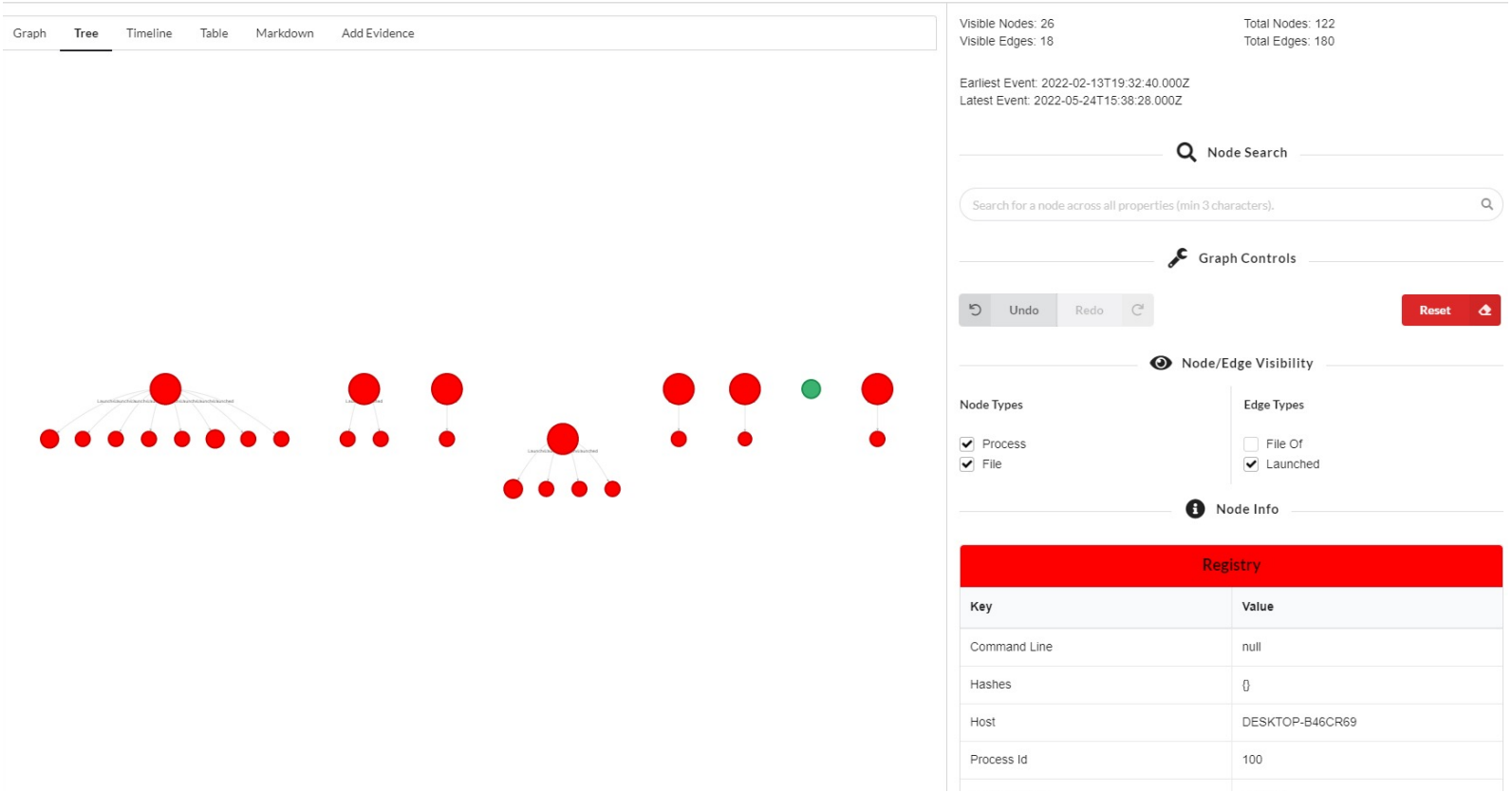
- Típus
- Tulajdonságok
- Irány
- Entitások közti kapcsolatokat ábrázolja



Saját példa:


external_reference
<id> 6
external_id CVE-2022-29072
source_name cve
value CVE-2022-29072
software
<id> 4
cpe cpe:2.3:a:7-zip:7-zip:*:*:*:*:*:*:*:*
id software--d0ec2afc-fee6-4695-8be0-9cdf079380a8
is_os false
name 7-zip
spec_version 2.1
type software
version 21.06 (x64)
port_scan
<id> 1
filtered_ports [22]
id port-scan--1aaa349e-07d2-4c5f-ae32-f12e8fd86c8c
open_ports [135,80,8080,443]
spec_version 2.1-custom
type port-scan
cvss2.0
https://s...
cve
refers_to
refers_to
refers_to
CVE-20...
has
7-zip
consists_of
2.1-cust...
characterizes
LABOR2...
vulnerability
<id> 5
description ** DISPUTED ** 7-Zip through 21.07 on Windows allows privilege escalation and command execution when a file with the .7z extension is dragged to the H...
Show all
id vulnerability--68ff5e6f-272b-48a2-b7bd-fe407fba8a4b
name CVE-2022-29072
spec_version 2.1
type vulnerability
refers_to
cvss3.1
mac_addr
<id> 0
id mac-addr--a299ee32-3f22-4546-a9c9-c03b758ca72b
spec_version 2.1
type mac-addr
value d2:fb:49:24:37:18
infrastructure
<id> 3
description Labor-gep
id infrastructure--bbbbeecb-bf51-4bd5-9aab-1028e87d6463
name LABOR213-02
spec_version 2.1
type infrastructure
consists_of
2.1
resolves_to
2.1
ipv4_addr
<id> 2
id ipv4-addr--419f6a85-863a-4891-958b-293f150b14ef
resolves_to_refs mac-addr--a299ee32-3f22-4546-a9c9-c03b758ca72b
spec_version 2.1
type ipv4-addr
value 10.3.13.110/24

Gráf vizualizálása



Incidensek

Miért tároljuk el?

Hogyan tároljuk el?

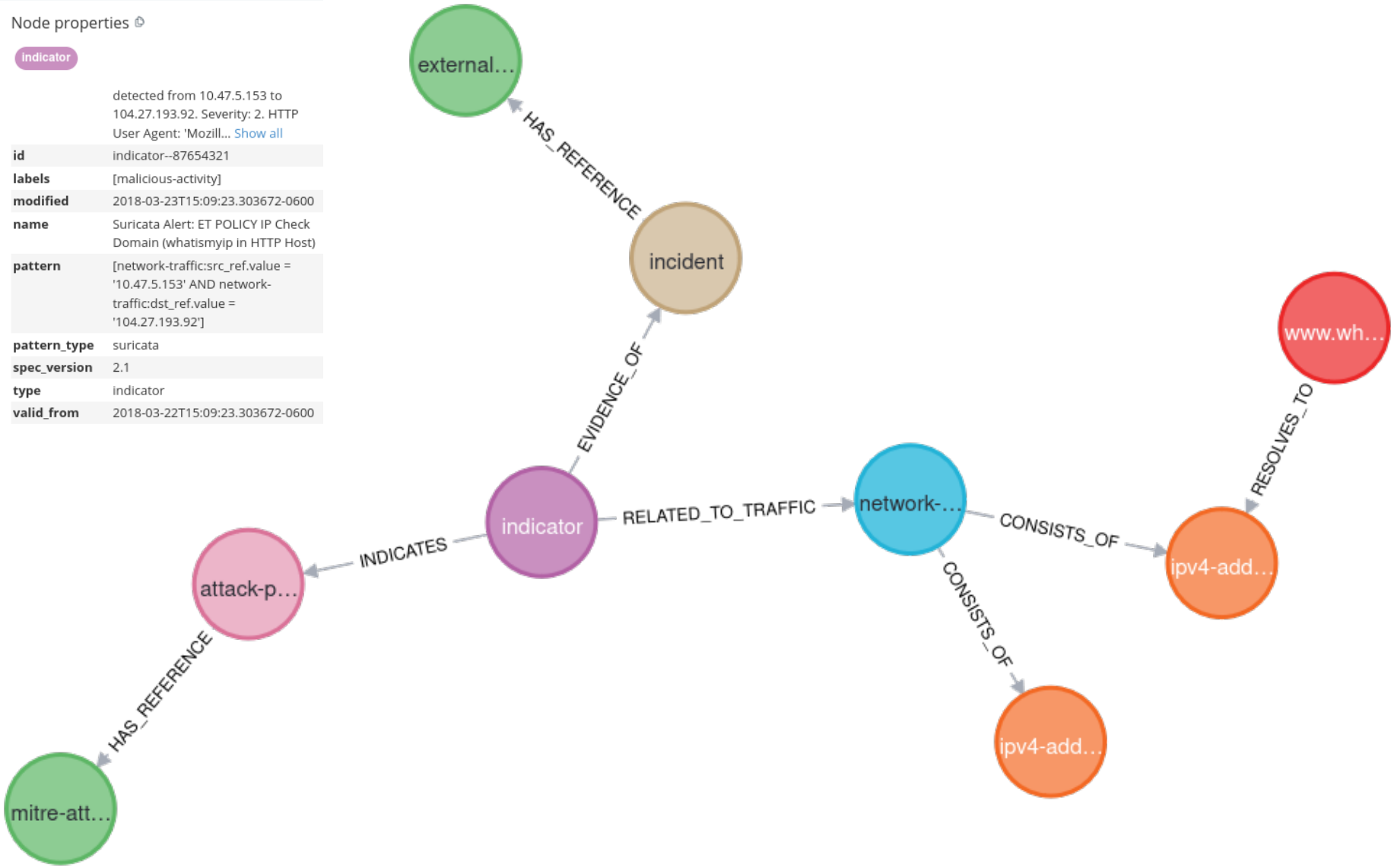
Mit hordoz magával?

- Indikátor

Suricata Alert


```
{
    "timestamp": "2018-03-23T15:09:23.303672-0600",
    "flow_id": 1594227117218106,
    "pcap_cnt": 1373851,
    "event_type": "alert",
    "src_ip": "10.47.5.153",
    "src_port": 63329,
    "dest_ip": "104.27.193.92",
    "dest_port": 80,
    "proto": "TCP",
    "tx_id": 0,
    "alert": {
      "action": "allowed",
      "gid": 1,
      "signature_id": 2008986,
      "rev": 7,
      "signature": "ET POLICY IP Check Domain (whatismyip in HTTP Host)",
      "category": "Attempted Information Leak",
      "severity": 2
    },
    "http": {
      "hostname": "www.whatismyip.com",
      "url": "/",
      "http_user_agent": "Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleW
      "http_content_type": "text/html",
      "http_method": "GET",
      "protocol": "HTTP/1.1",
      "status": 301,
      "redirect": "https://www.whatismyip.com/",
      "length": 180
    },
    "app_proto": "http",
    "flow": {
      "pkts_toserver": 7,
      "pkts_toclient": 8,
      "bytes_toserver": 1192,
      "bytes_toclient": 1598,
      "start": "2018-03-23T15:09:23.153914-0600"
    }
  },
```

Incidens gráfként



Fejlesztés alatt..

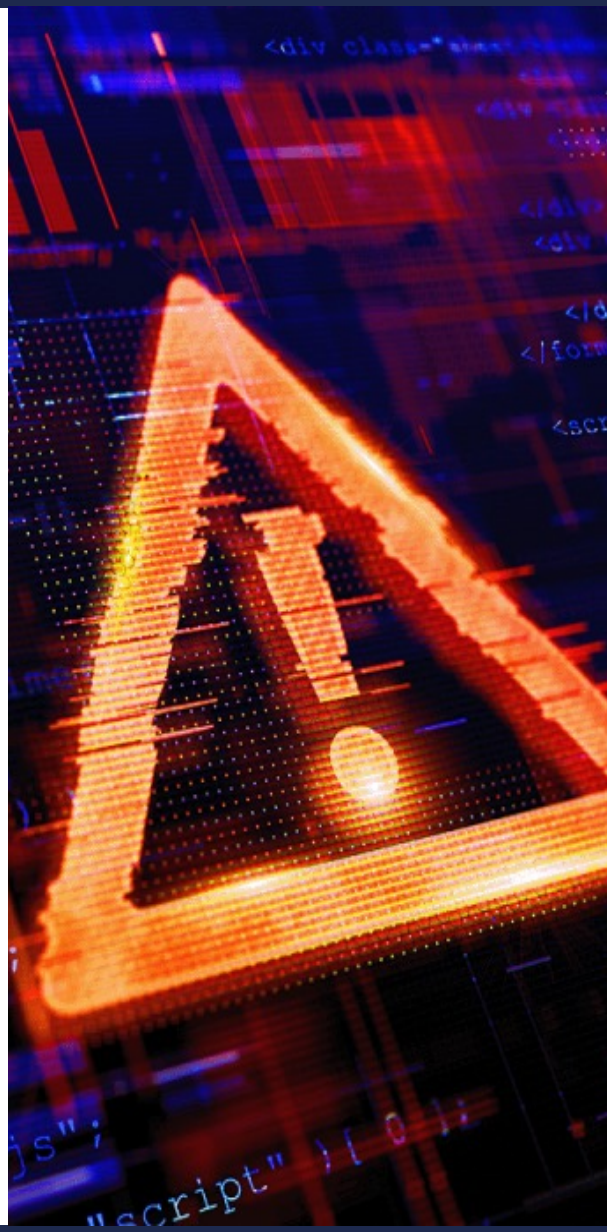
- Geolokációs adatok
  - Támadók profilozása
- Egy közös grafikus felület
  - Amiről menedzselni lehet a projekt komponenseit

ipstack

Whois
Identity for everyone

Jövőbeli tervek és use-case-ek

- A sérülékenységek ábrázolásán túl…
  - Kockázatelemzés a sérülékenységek mentén kialakítható támadási útvonalak alapján
  - Logadatok beépítése a gráfba és azok elemzése,
  - Támadók profilozása honeypot logok alapján,
  - A grafikus és felhasználói felület továbbfejlesztése



Ha csatlakozol…

Milyen képességeket lehet elsajátítani?

Összegzés

A projekt témája:

- gráfvizualizáció
- adatok ➢ grafikonok, diagramok

A projekt célja:

- *IT biztonsági elemzők munkájának segítése*
- *A SOC komponenseinek optimalizálása*

Köszönjük a figyelmet!