SECURITY DAYS

SAUGUMO OPERACIJŲ AUTOMATIZAVIMAS: NUO IDĖJOS IKI ĮRANKIO

Marius Urkis - NRD Cyber Security
CSIRT/SOC architektas

Rugsėjo 5 d. 2024
KIBERNETINIO SAUGUMO KONFERENCIJA
esd.eset.lt

NRD Cyber Security

Threat Hunting

Saugumo operacijų automatizavimas: nuo idėjos iki įrankio

Marius Urkis
mu@nrdcs.lt

NRD Cyber Security

Marius Urkis

CSIRT/SOC architect

- Marius Urkis yra CSIRT/SOC architektas, turintis daugiau nei 20 metų patirties kibernetinio saugumo srityje.

- Vadovauja NRD CIRT bei specializuojasi:
  - Incidentų aptikimo srityje;
  - Triažo, analizės ir atkūrimo srityse;
  - Pažeidžiamumų bei atitikties valdymo srityse;
  - Kuriant CSIRT įrankius ir sprendimus.

- Prieš pradėdamas dirbti NRD Cyber Security, Marius 15 metų vadovavo LITNET CERT, kuri teikė kibernetinio saugumo paslaugas akademinėms mokslinių tyrimų organizacijoms. Jis vadovavo pirmosios Baltijos šalyse CSIRT įkūrimui ir valdymui.

Specializacija

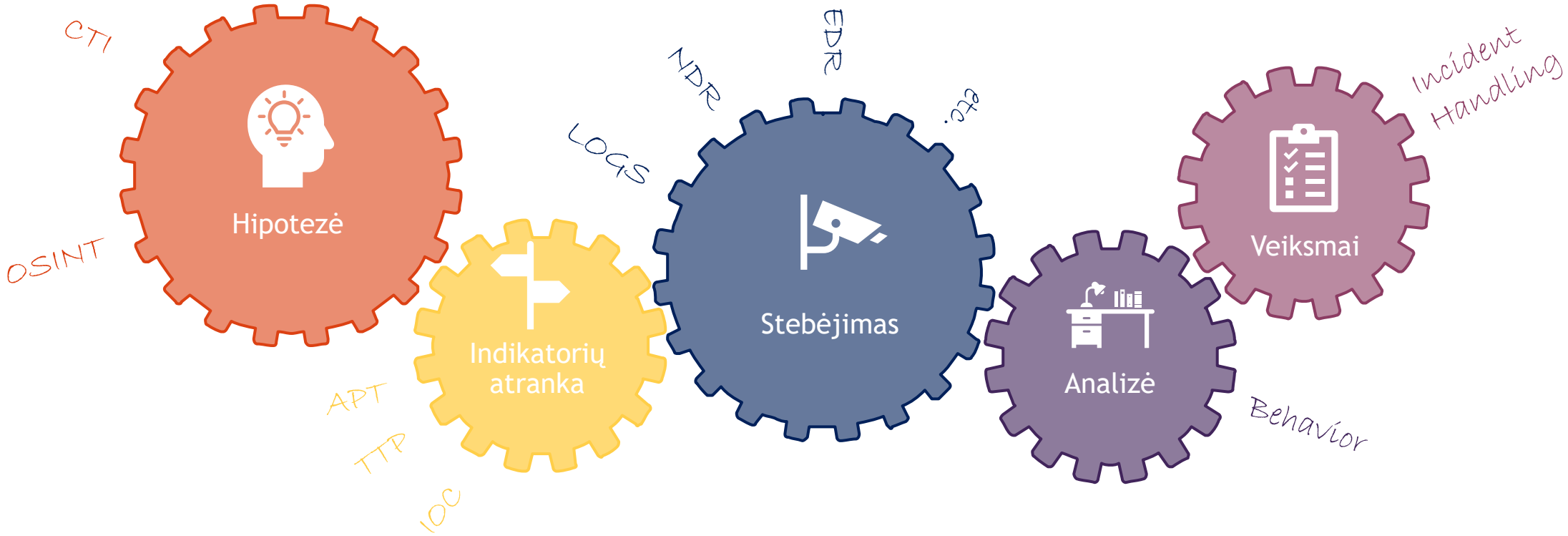
- SOC/CSIRT steigimas ir veikla;
- Nacionalinės kritinės svarbos informacinės infrastruktūros identifikavimas;
- Pažeidžiamumų ir atitikties valdymas;
- Kriminalistiniai tyrimai;
- Incidentų valdymas.

Sertifikatai

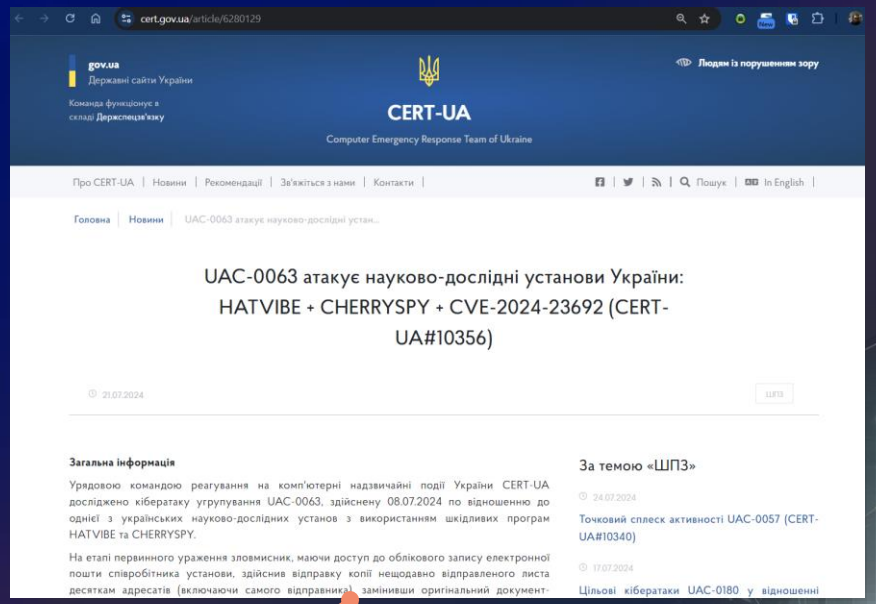
Sertifikuotas SIM3 auditorius I Sertifikuotas SOC-CMM vertintojas

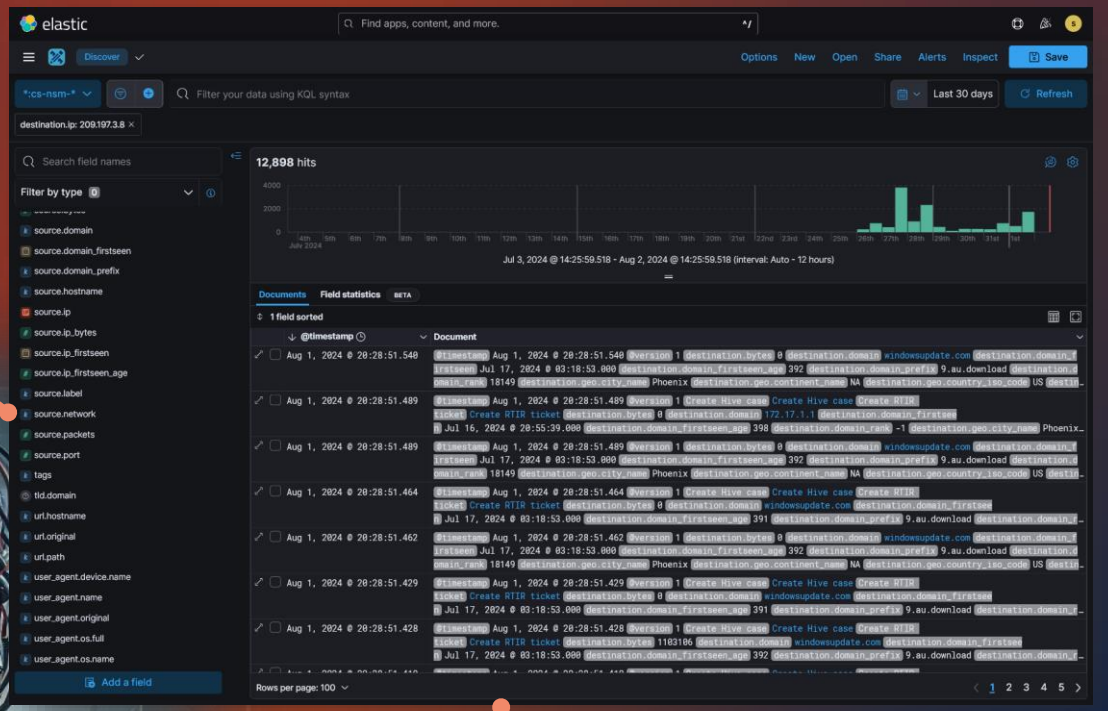
Kas yra grėsmių medžioklė?

Proaktyvi paieška → Kiber. grėsmių → Tinkle, aplinkoje → Anksčiau neaptiktų



Kaip tai galėtų veikti?





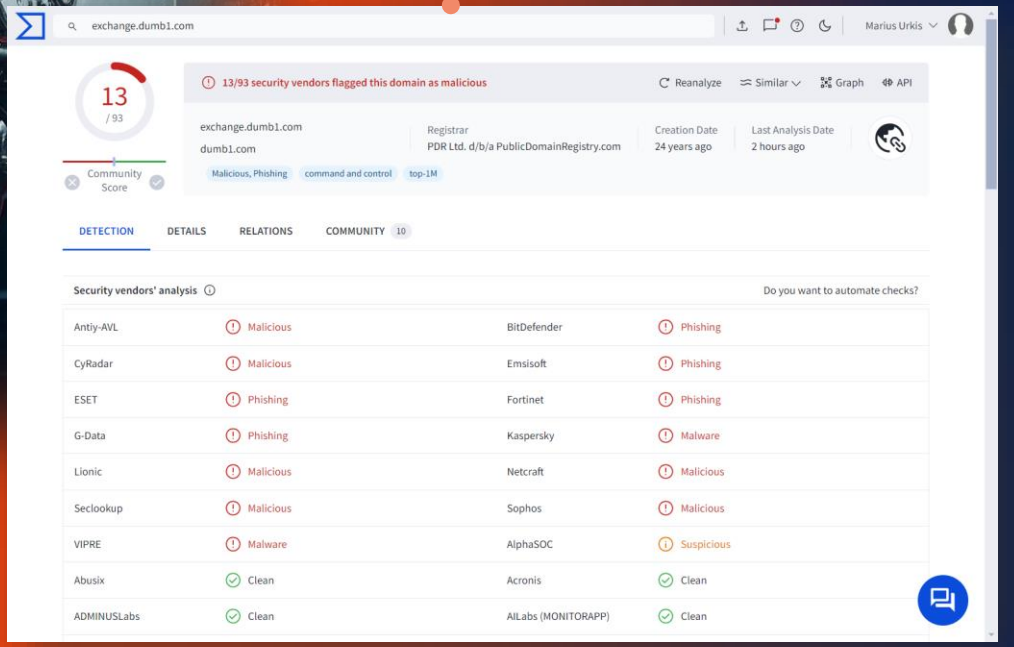
Індикатори кіберзагроз

Файли:

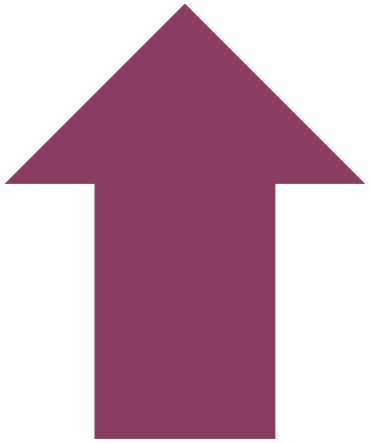
```
197e86b76a41f154b64e092f7cc3b306    6c439e62fb404e9095392878ef32ffce18ce6155a1510f400540924
81cdcda59c86f8aa636810e4a085d673    f9baa77117f5a058461e859efc67c8ce1ac205d1536326e01a030ab
7a2a8c002a5e22c6231885e1ccf82bd1    593ca6d639f7c3e99db768b318b765e7585496debfde553dc1df03f
7f865b65a82dcb18385644e0fd894727    259619899c60aa46df4f83558606813c79927c141bbf4b21bbf07b2
33c3e4599ad678133905e6c1589c12d2    e6daa00e095948acfc176d71c5bf667a0403e5259653ea5ac8950ae
d618720afd0ee49601f7933c414ffbb5    bcdbe035001af9d2cc173e975fa0b13b133e613b7d9b6e90df86672
8e1b29046c7f5bd1ddd4f549e2555592    f4ada2b858c84da8b53c08ce4579f8b5b5df25e0d0f17ee0b48e10c
d84043b72bdceb92b2d60c2725bd674f    93322be0785556e627d2b09832c18e39c115e6a6fbff64b1e590e1d
34ced721349626ce81c11693b9243c19    a171e9c413518750806ae094e32f15791d4193229cc598642760af5
d0c3b49e788600ff3967f784eb5de973    332d9db35daa83c5ad226b9bf50e992713bc6a69c9ecd52a1223b81
8159abd281783e0ae601afce3b7d23b1    48a30083f115ca0d359afc175cf942367207a73fdda28778e2b2645
```

Мережеві:

```
hXXp://trust-certificate[.]net/setup.php
hXXp://trust-certificate[.]net/tmp/379.zip
hXXps://enrollmentdm[.]com:443
trust-certificate[.]net   2024-07-09  @namecheap.com
enrollmentdm[.]com    2024-05-13  @namecheap.com
185.158.248[.]198 RO  @m247.com
193.124.65[.]97   RU  @mtw.ru
45.136.198[.]184
5.45.70[.]178
hXXp://45.136.198[.]184/connect.php
hXXp://45.136.198[.]184/input.php
hXXp://45.136.198[.]184/output.php
hXXp://5.45.70[.]178/RemoteAssistanceSvc.hta
```

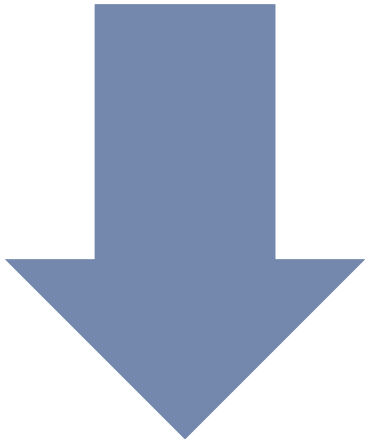


Mūsų įrankiai: atviras kodas



Privalumai

- Prieiga prie kodo
- Galimybė pritaikyti
- Bendruomenės indėlis
- Nemokama



Trūkumai

- Reikalingos žinios
- Aptarnavimo stoka

ail project

RT | IR

Lookyloo

MISP Threat Sharing

T-POT

INTELMQ

GreedyBear

OpenCTI By Filigran

cape

Intel owl

artemis

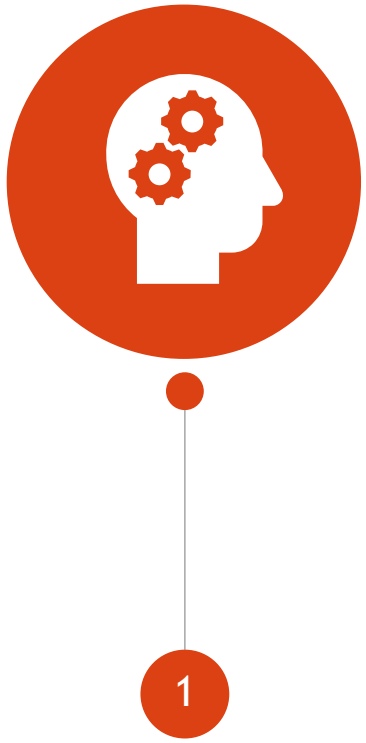
Imkimės konstruoti robotą!

IDĖJA

ĮRANKIAI

REALIZACIJA

Eskizas realizacijai

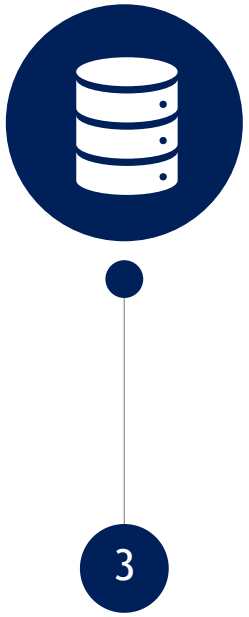


1

Surinkti informaciją

2

Įvertinti CTI duomenis ir atrinkti IOC



3

Peržiūrėti žurnalus

4

Registruoti incidentą

5

Atlikti analizę

APT

Žingsnis 1:

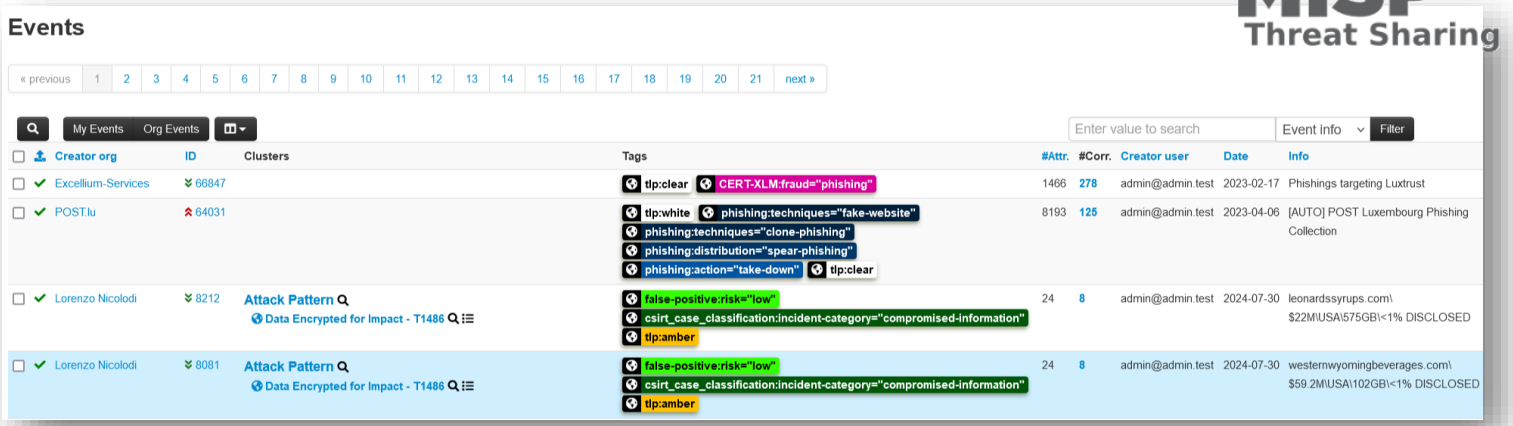
Surinkti informaciją

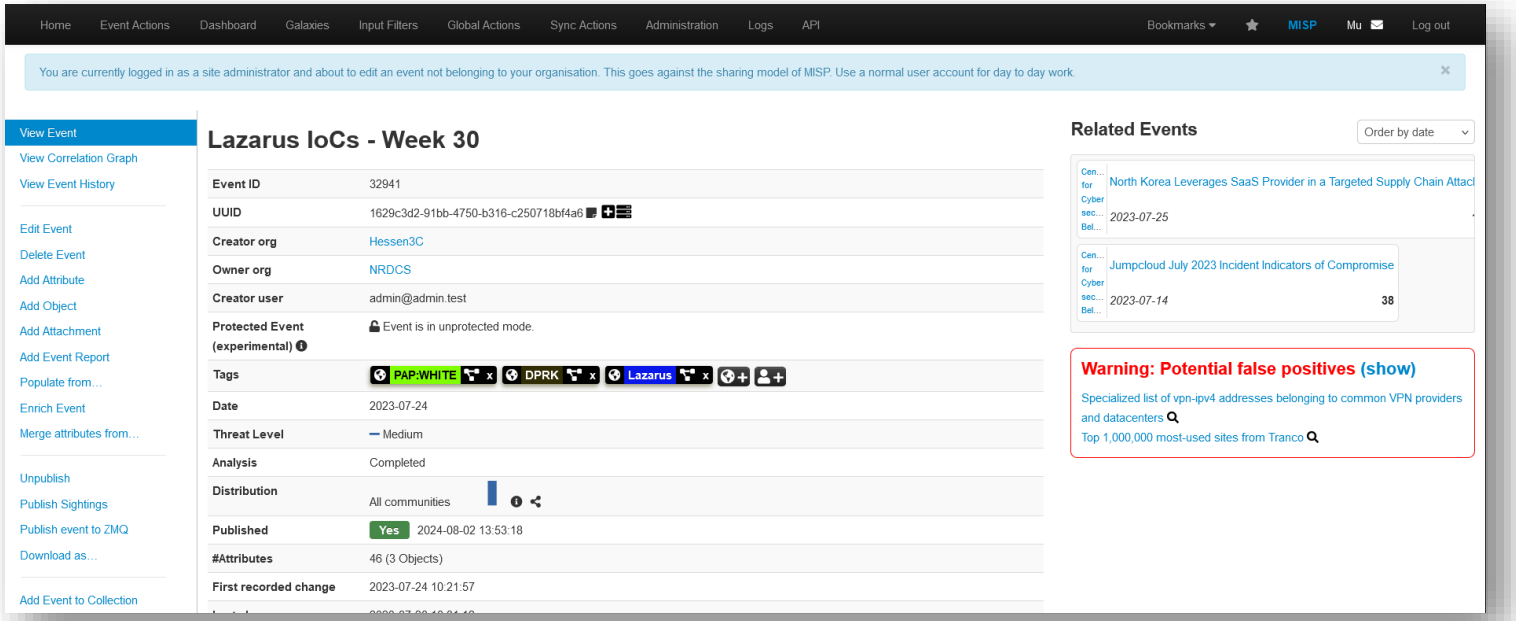
CTI rinkimas

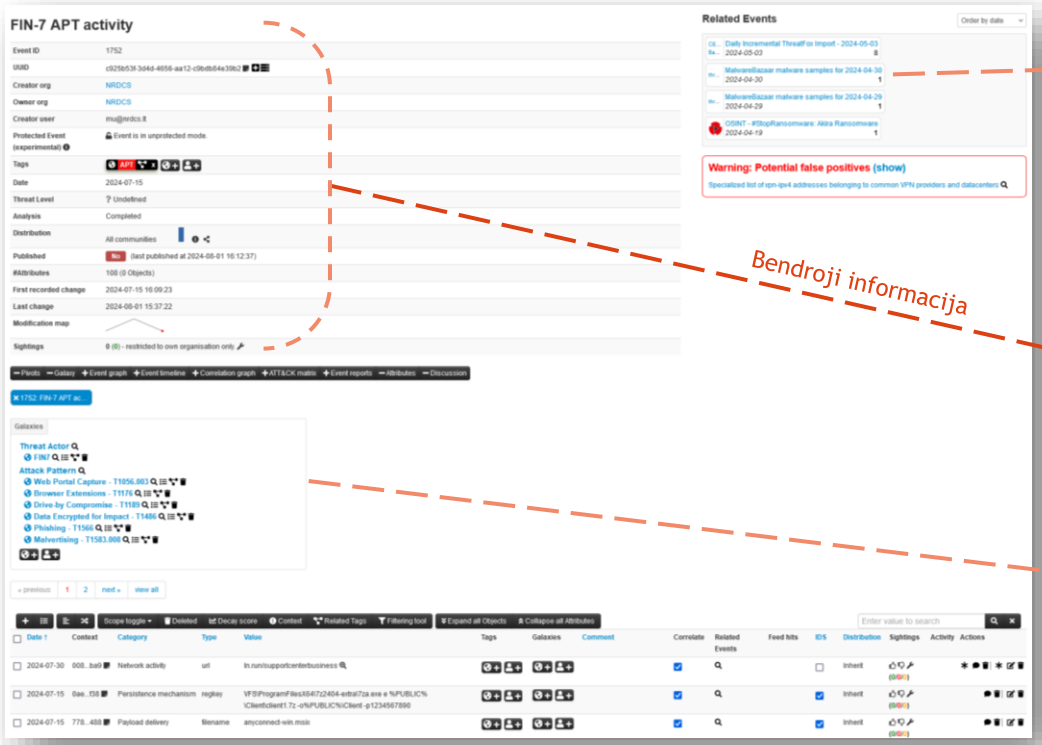
- Įrankis:
  - MISP, Malware Information Sharing Platform
  - https://github.com/MISP/MISP
- CTI valdymo priemonė
- Sukurtas dalinimuisi
- Kibernetinių grėsmių duomenys bei kontekstas
- Bendruomenės pajėgumai

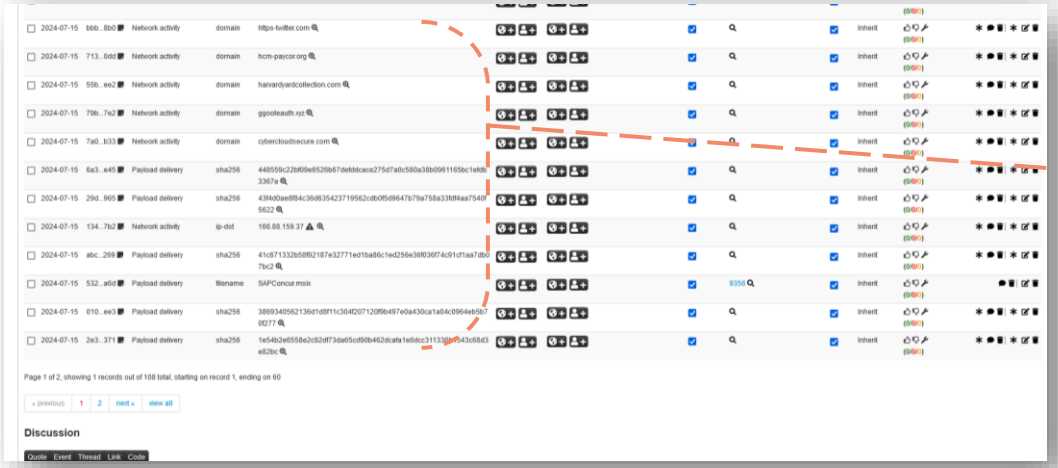
Cyber SOC

- REST API
  - https://www.misp-project.org/openapi/









Bendroji informacija

Taksonomija, kontekstas

Indikatoriai

Koreliacija ir false-positive požymiai

FIN-7 APT activity

Event ID	1752
UUID	c925b53f-3d4d-4656-aa12-c9bdb84e39b2
Creator org	NRDCS
Owner org	NRDCS
Creator user	mu@nrdcs.lt
Protected Event (experimental)	Event is in unprotected mode.
Tags	APT
Date	2024-07-15

Related Events

Order by date

- Daily Incremental ThreatFox Import - 2024-05-03 — 2024-05-03 — 8
- MalwareBazaar malware samples for 2024-04-30 — 2024-04-30 — 1
- MalwareBazaar malware samples for 2024-04-29 — 2024-04-29 — 1
- OSINT - #StopRansomware: Akira Ransomware — 2024-04-19 — 1

Warning: Potential false positives (show)

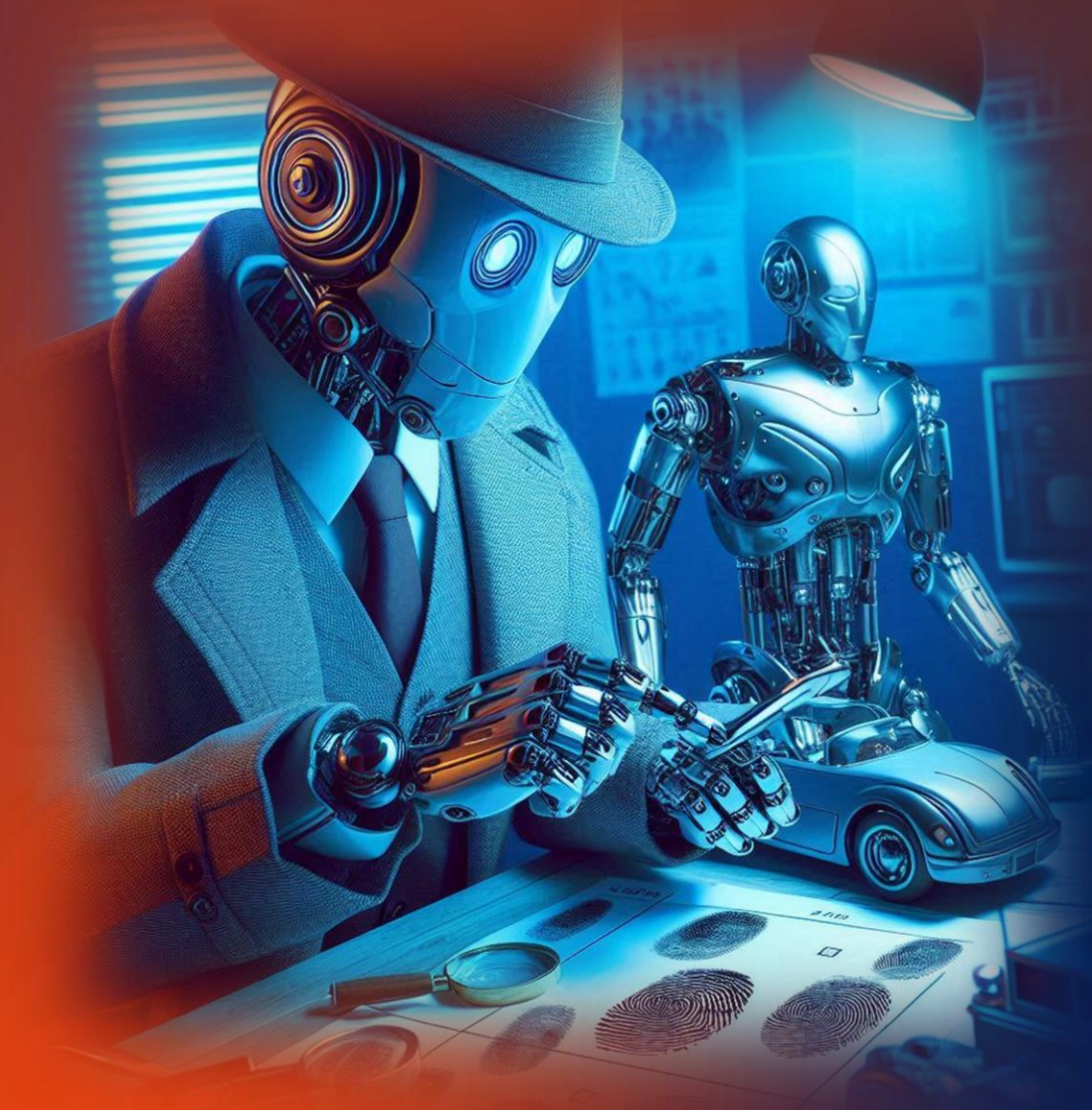
Specialized list of vpn-ipv4 addresses belonging to common VPN providers and datacenters

1752: FIN-7 APT ac...

Galaxies

- Threat Actor
  - FIN7
- Attack Pattern
  - Web Portal Capture - T1056.003
  - Browser Extensions - T1176
  - Drive-by Compromise - T1189
  - Data Encrypted for Impact - T1486
  - Phishing - T1566
  - Malvertising - T1583.008

2024-07-15	87d...dfd	Network activity	ip-dst	103.113.70.142
2024-07-15	743...5ff	Network activity	domain	westlaw.top
2024-07-15	2c4...9b9	Network activity	domain	thomsonreuter.pro
2024-07-15	0df...ddd	Network activity	domain	thomsonreuter.info

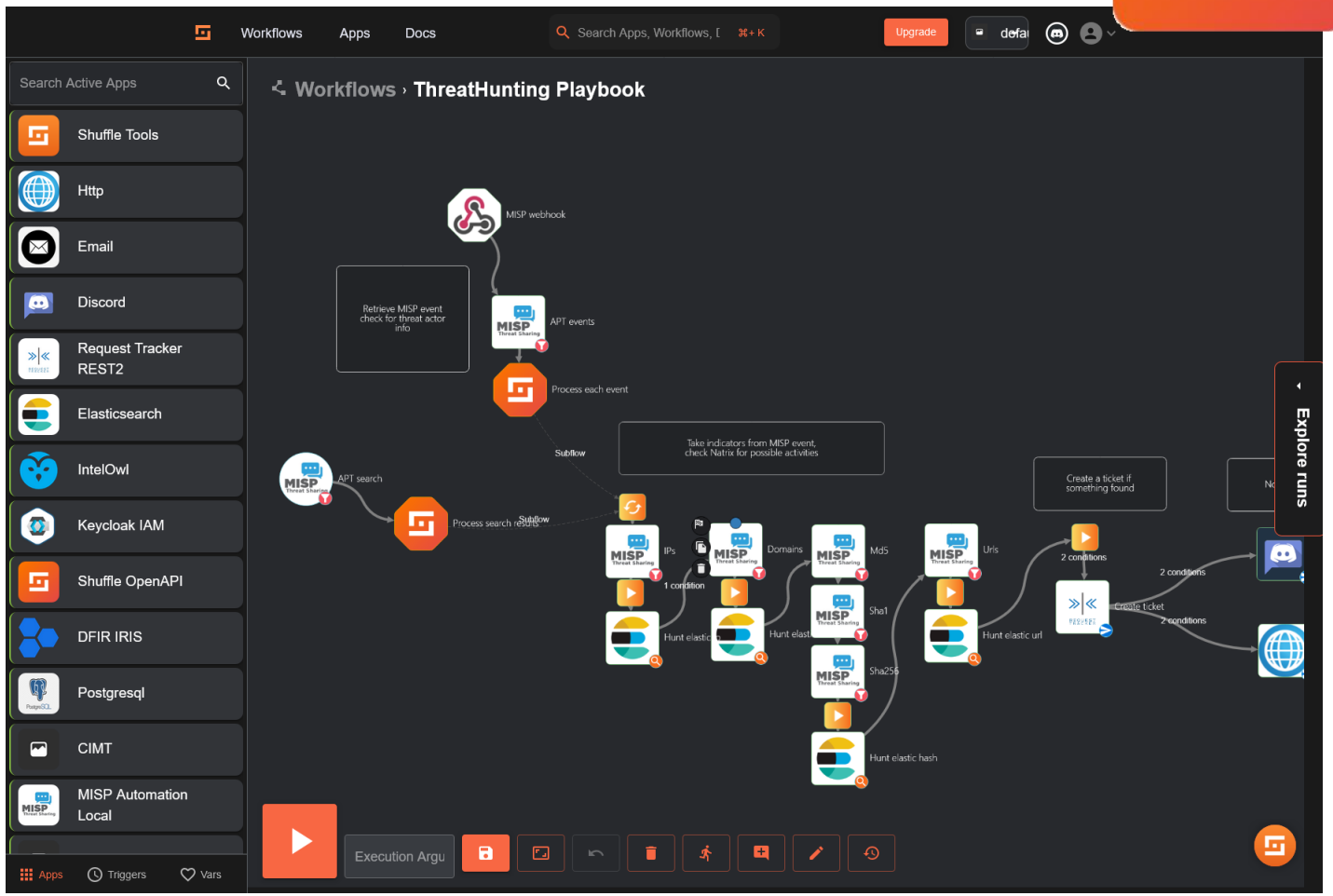


Žingsnis 2:

Įvertinti CTI duomenis ir atrinkti IOC

Duomenų ir indikatorių atrinkimas

- Įrankis:
  - Shuffle, atviro kodo SOAR
  - https://github.com/Shuffle/Shuffle
- Apjungia
  - Aplikacijas, sąlygas
  - Į automatizuotas veiksmų sekas
- Savybės
  - Workflow dizaineris
  - Sąlygos: laiko grafikas, webhook
  - Aplikacijų kūrimas
  - OpenAPI importavimas



Persiųsti MISP srautą į Shuffle apdorojimui

CTI champion

ZeroMQ

Optional	Plugin.ZeroMQ_enable	true	Enables or disables the pub/sub feature of MISP. Make sure that you inst
Optional	Plugin.ZeroMQ_host	misp-zeromq	The host that the pub/sub feature will use.
Optional	Plugin.ZeroMQ_port	50000	The port that the pub/sub feature will use.
Optional	Plugin.ZeroMQ_username		The username that client need to use to connect to ZeroMQ.
Optional	Plugin.ZeroMQ_password	*****	The password that client need to use to connect to ZeroMQ.
Optional	Plugin.ZeroMQ_redis_host	redis	Location of the Redis db used by MISP and the Python PUB script to que
Optional	Plugin.ZeroMQ_redis_port	6379	The port that Redis is listening on.
Optional	Plugin.ZeroMQ_redis_password	*****	The password, if set for Redis.
Optional	Plugin.ZeroMQ_redis_database	1	The database to be used for queuing messages for the pub/sub function
Optional	Plugin.ZeroMQ_redis_namespace	mispq	The namespace to be used for queuing messages for the pub/sub functi
Optional	Plugin.ZeroMQ_include_attachments	false	Enable this setting to include the base64 encoded payloads of malware-
Optional	Plugin.ZeroMQ_event_notifications_enable	true	Enables or disables the publishing of any event creations/edits/deletions
Optional	Plugin.ZeroMQ_object_notifications_enable	false	Enables or disables the publishing of any object creations/edits/deletions

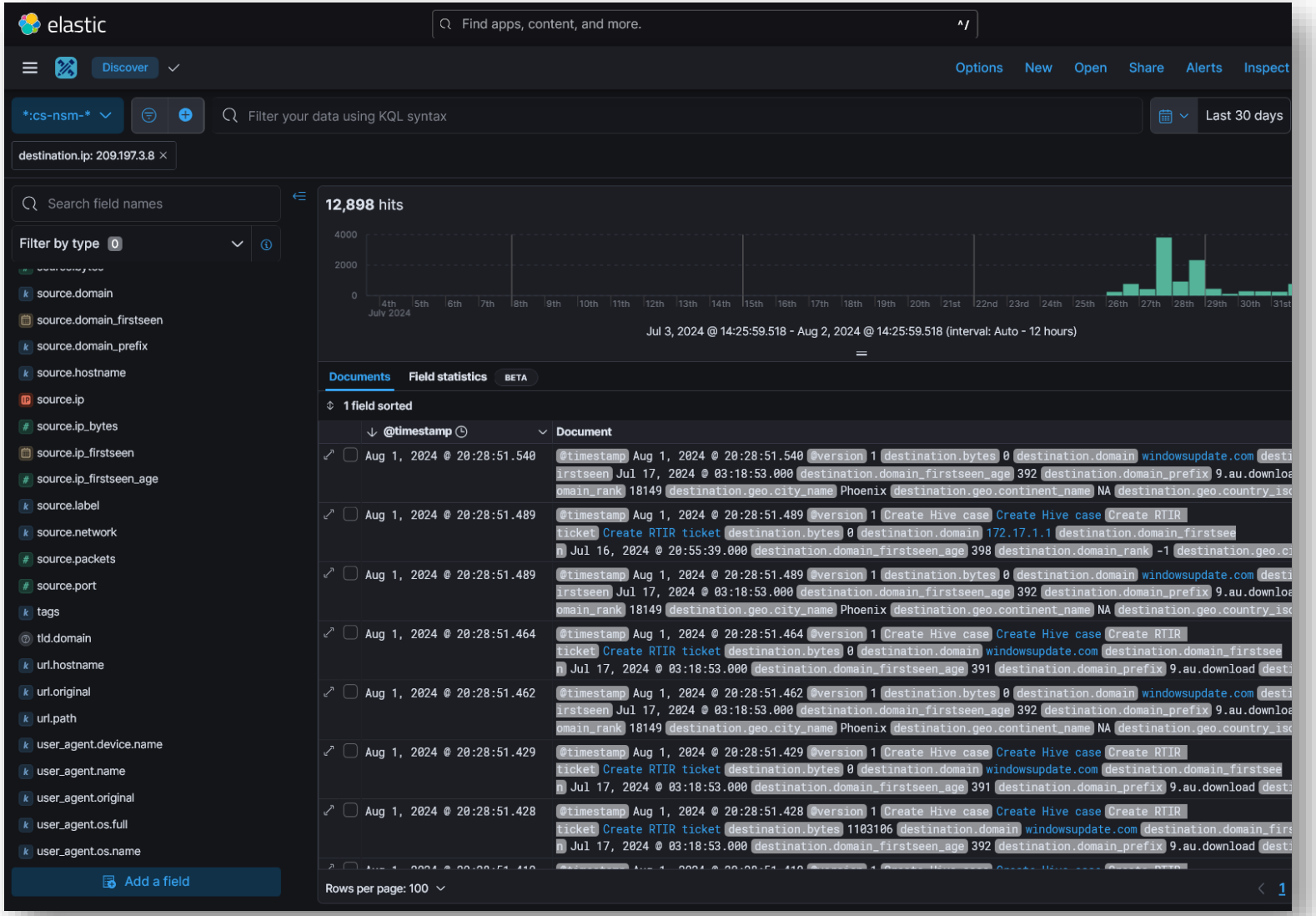

```
{
  "returnFormat": "json",
  "uuid": "$exec.Event.uuid",
  "tag": "misp-galaxy:threat-actor=%",
  "last": "1d",
  "limit": "10",
  "published": true
}
```

Žingsnis 3:

Peržiūrėti žurnalus

Paieška NDR įrašų istorijoje

- NDR - Network Detection and Response
  - ElasticSearch
  - https://www.elastic.co/guide/en/elasticsearch/reference/current/docs.html



Automatizuojame: surinkti ir ieškoti

Atrinkti IP adresus, pažymėtus IDS naudojimui, ignoruoti atitinkančius Warning List

Filters | Math | Python | + Autocomplete

```
{
  "returnFormat": "json",
  "type": "ip-dst",
  "to_ids": true,
  "enforceWarninglist": true,
  "uuid": "$misp_event.uuid"
}
```

Ištraukti agreguotus ir filtruotus duomenis

History: Last 60 days?

Filters | Math | Python | + Autocomplete

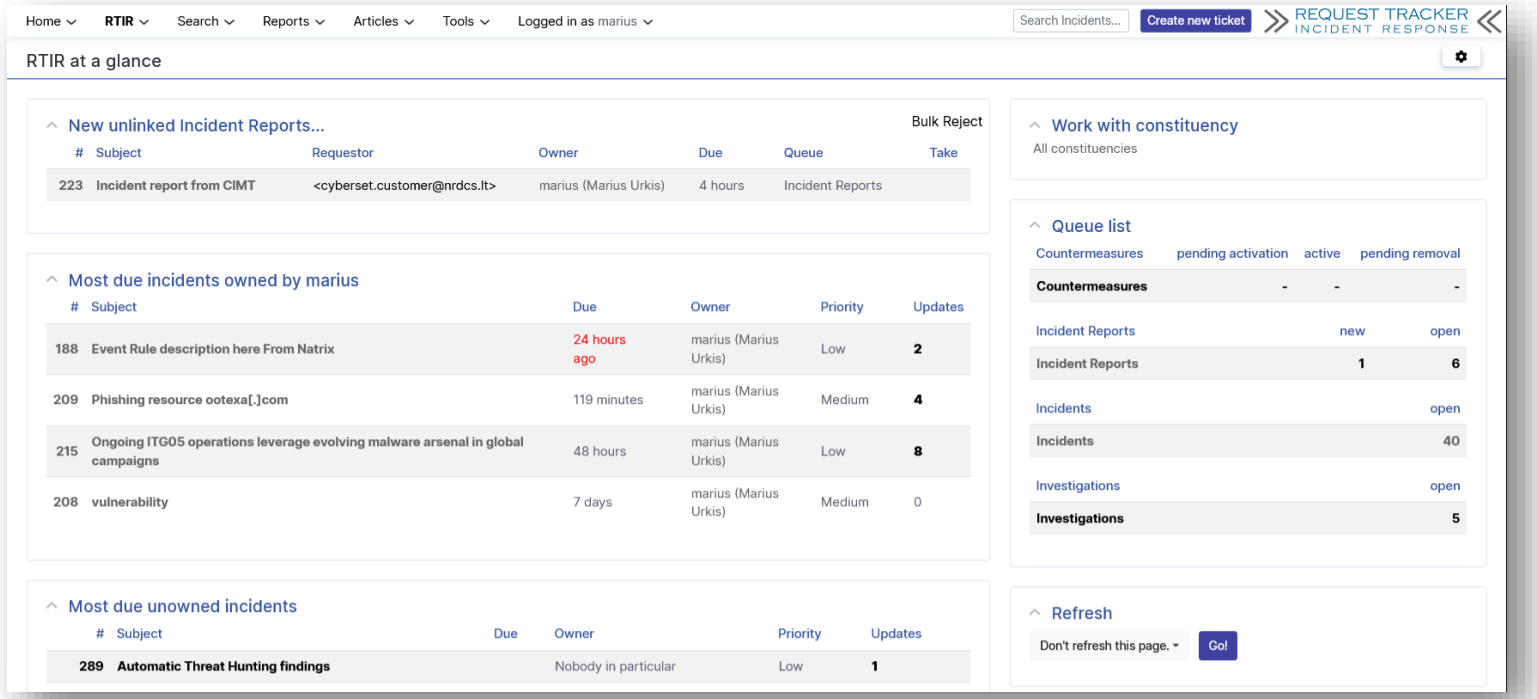
```
{
"aggs": {"0": {"terms": {"field": "observer.name","order":
  {"_count": "desc"},"size":3,"shard_size": 25},
  "aggs": {"1": {"terms": {"field": "source.ip","order": {"_count":
    {"multi_terms":{"terms": [{"field": "destination.ip"},{"field":
    ,"size": 5,"shard_size": 25}}}}}},
"sort": [{"@timestamp": {"order": "desc","unmapped_type": "boolean"}
  "size": 0,
"query": {"bool": $filter_ip.message
}
}
```

Žingsnis 4:

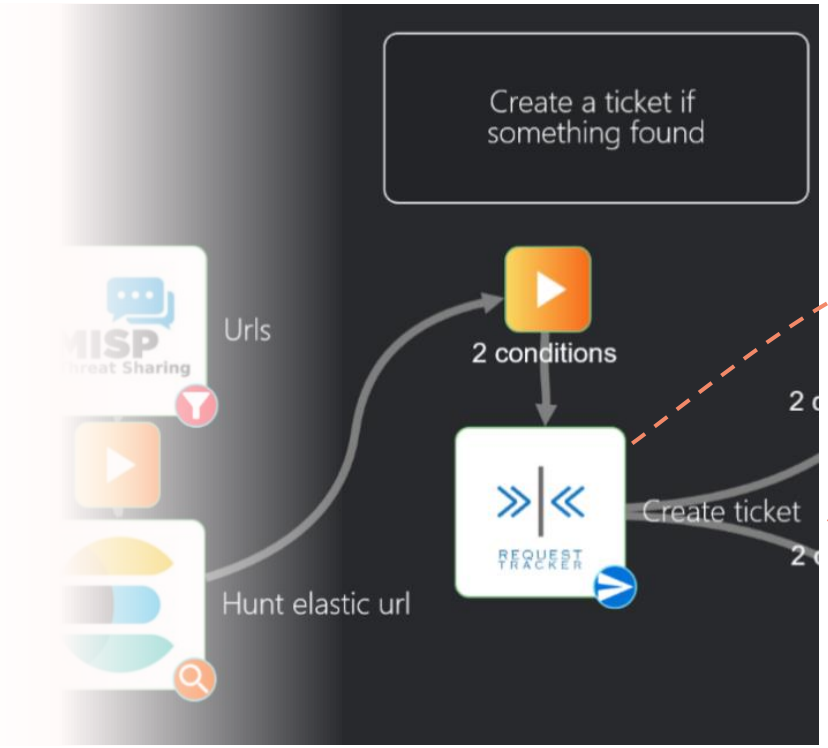
Registruoti incidentą

Registravimas: incidentai ir bilietų sistema

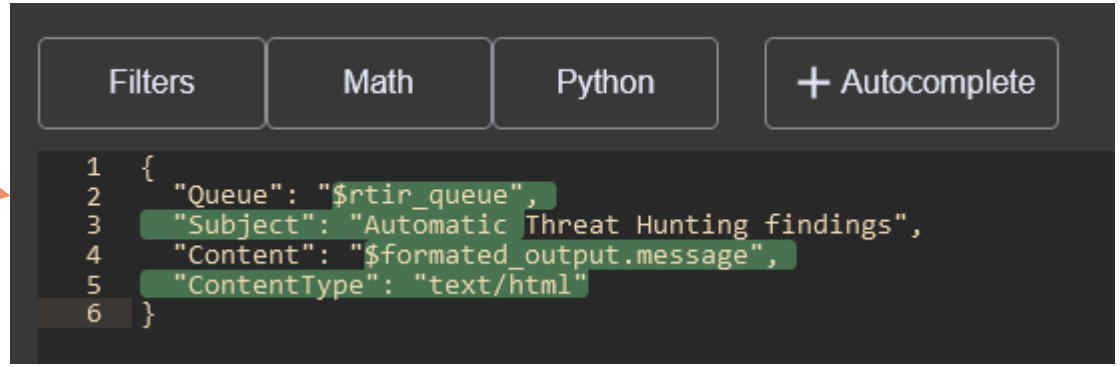
- Įrankis:
  - Ticketing System
  - Request Tracker for Incident Response
  - https://github.com/bestpractical/rt
  - https://github.com/bestpractical/rtir
- Sąvybės
  - Plečiamumas
    - Callbacks
    - Overlays
    - Extensions (https://github.com/bestpractical)
  - Automatiniai veiksmai
    - Vidinės logikos veiksmai (scrips)
    - REST API (https://docs.bestpractical.com/rt/5.0.7/RT/REST2.html)
    - CLI tools



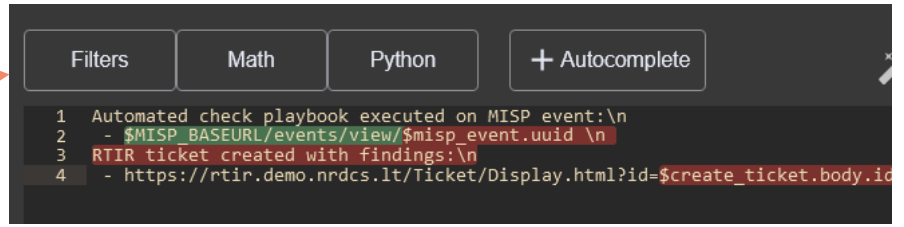
„Ticketing“ automatizavimas



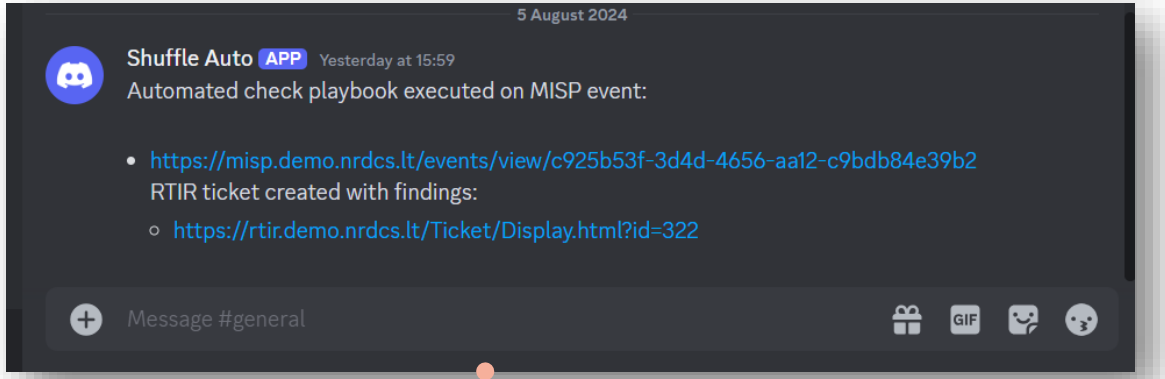
Registruoti incidentą sistemoje

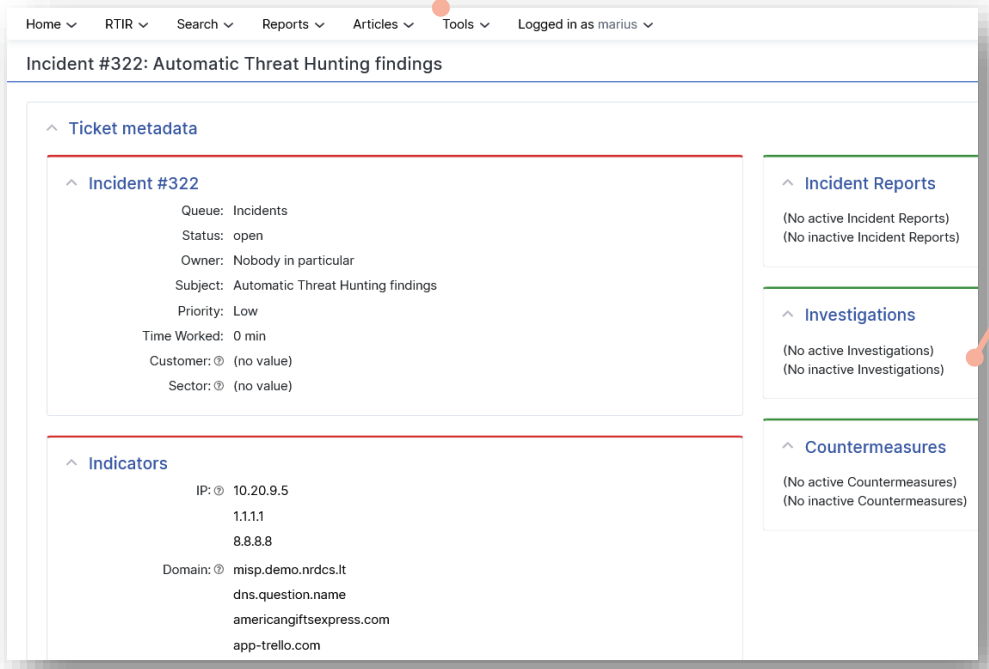


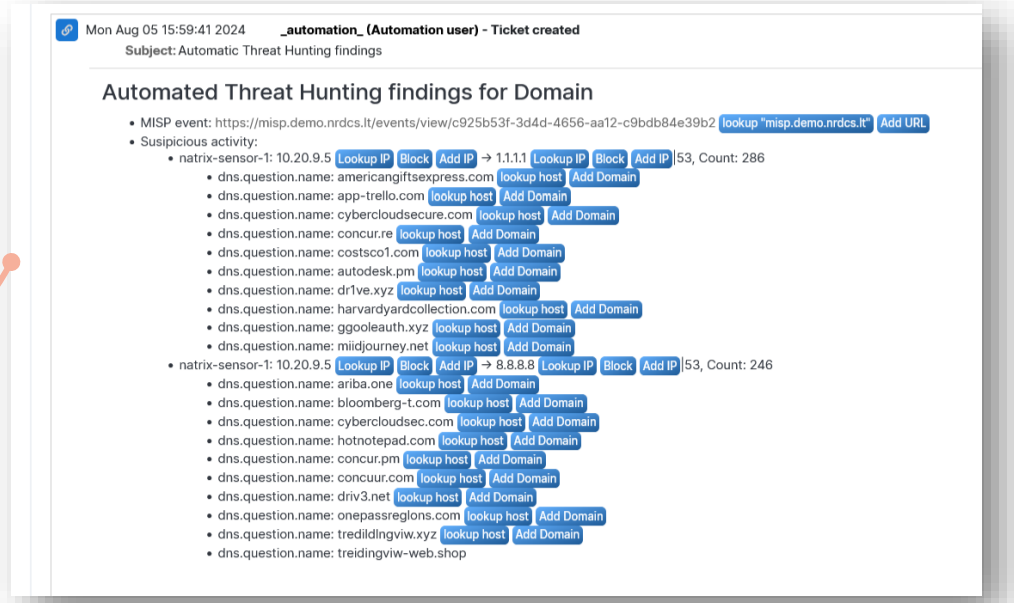
Informuoti analitikus - Discord, Teams, t.t.



Rezultatas


5 August 2024
Shuffle Auto APP Yesterday at 15:59
Automated check playbook executed on MISP event:
https://misp.demo.nrdcs.lt/events/view/c925b53f-3d4d-4656-aa12-c9bdb84e39b2
RTIR ticket created with findings:
https://rtir.demo.nrdcs.lt/Ticket/Display.html?id=322
Message #general
GIF

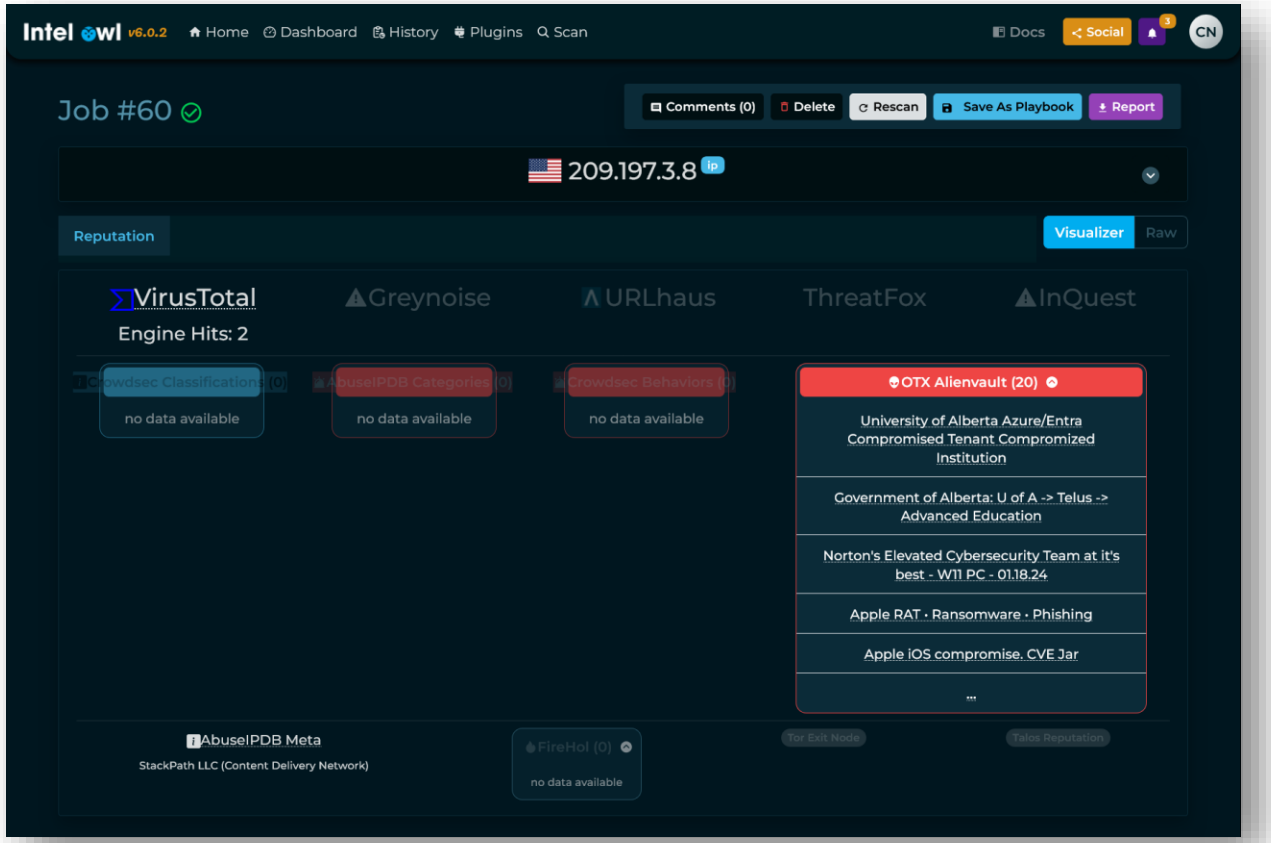

Home
RTIR
Search
Reports
Articles
Tools
Logged in as marius
Incident #322: Automatic Threat Hunting findings
Ticket metadata
Incident #322
Queue: Incidents
Status: open
Owner: Nobody in particular
Subject: Automatic Threat Hunting findings
Priority: Low
Time Worked: 0 min
Customer: (no value)
Sector: (no value)
Indicators
IP: 10.20.9.5
1.1.1.1
8.8.8.8
Domain: misp.demo.nrdcs.lt
dns.question.name
americangiftsexpress.com
app-trello.com
Incident Reports
(No active Incident Reports)
(No inactive Incident Reports)
Investigations
(No active Investigations)
(No inactive Investigations)
Countermeasures
(No active Countermeasures)
(No inactive Countermeasures)


Mon Aug 05 15:59:41 2024 _automation_ (Automation user) - Ticket created
Subject: Automatic Threat Hunting findings
Automated Threat Hunting findings for Domain
MISP event: https://misp.demo.nrdcs.lt/events/view/c925b53f-3d4d-4656-aa12-c9bdb84e39b2 lookup "misp.demo.nrdcs.lt" Add URL
Susipicious activity:
natrix-sensor-1: 10.20.9.5 Lookup IP Block Add IP → 1.1.1.1 Lookup IP Block Add IP 53, Count: 286
dns.question.name: americangiftsexpress.com lookup host Add Domain
dns.question.name: app-trello.com lookup host Add Domain
dns.question.name: cybercloudsecure.com lookup host Add Domain
dns.question.name: concur.re lookup host Add Domain
dns.question.name: costsco1.com lookup host Add Domain
dns.question.name: autodesk.pm lookup host Add Domain
dns.question.name: dr1ve.xyz lookup host Add Domain
dns.question.name: harvardyardcollection.com lookup host Add Domain
dns.question.name: ggooleauth.xyz lookup host Add Domain
dns.question.name: miidjourney.net lookup host Add Domain
natrix-sensor-1: 10.20.9.5 Lookup IP Block Add IP → 8.8.8.8 Lookup IP Block Add IP 53, Count: 246
dns.question.name: ariba.one lookup host Add Domain
dns.question.name: bloomberg-t.com lookup host Add Domain
dns.question.name: cybercloudsec.com lookup host Add Domain
dns.question.name: hotnotepad.com lookup host Add Domain
dns.question.name: concur.pm lookup host Add Domain
dns.question.name: concuur.com lookup host Add Domain
dns.question.name: driv3.net lookup host Add Domain
dns.question.name: onepassreglons.com lookup host Add Domain
dns.question.name: tredildlngviw.xyz lookup host Add Domain
dns.question.name: treidingviw-web.shop

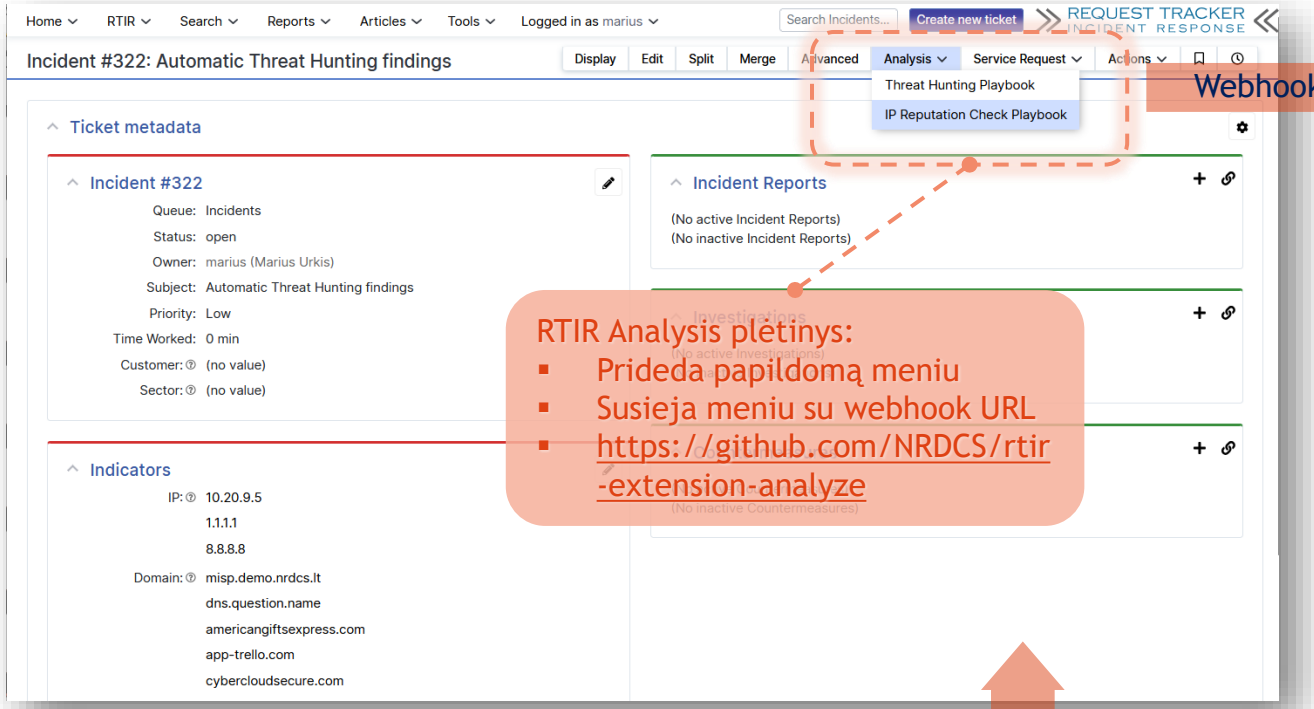
Žingsnis 5:
Atlikti analizę

Analizė

- Įrankis:
  - IntelOwl
  - https://github.com/intelowlproject/IntelOwl
  - Indikatoriai: IP, FQDN, URL, hash, t.t
  - Papildyti grėsmių žvalgybos informacija
  - Apjungia analizatorius į atlikimo eigas (playbook)
  - REST API
    - https://intelowl.readthedocs.io/en/latest/Redoc.html



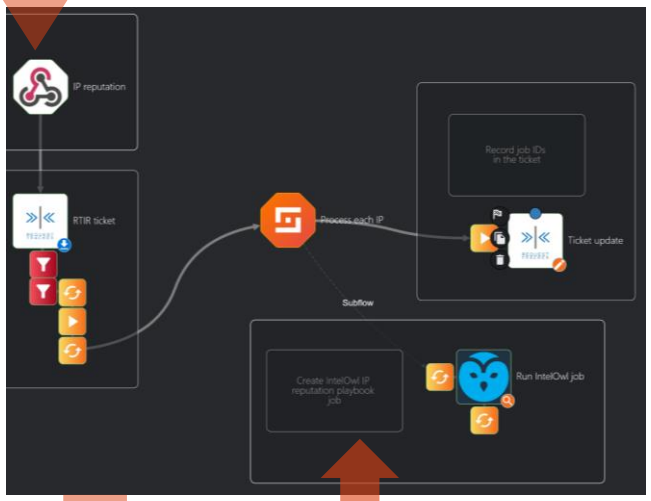
Pridėkim RTIR įrankiui analitines funkcijas



RTIR Analysis plėtinys:

- Prideda papildomą meniu
- Susieja meniu su webhook URL
- https://github.com/NRDCS/rtir-extension-analyze

Webhook kreipinys



Intel owl

Rezultatai pridedami prie incidento

VirusTotal · URLhaus by ABUSE.ch · GREY NOISE · AbuseIPDB · ThreatFox · Tor · CrowdSec · CISCO Talos · OPEN THREAT EXCHANGE

Analizės rezultatai

Tue Jul 30 17:22:09 2024 **_automation_ (Automation user) - Comments added**

Automated analysis report from IntelOwl

URL: https://intelowl.demo.nrdcs.lt/api/jobs/58 lookup "intelowl.demo.nrdcs.lt" Add URL

- ThreatFox Report, retrieved at: **2024-07-30T10:34:16.658589Z**
  - **Your search did not yield any results**
- TOR Report, retrieved at: **2024-07-30T10:34:17.118417Z**
  - TOR Exit Node: **False**
- Crowdsec Report, retrieved at: **2024-07-30T10:34:16.645006Z**
  - IP: **185.191.126.213** Lookup IP Block Add IP
  - Reputation: **malicious**
  - Confidence: **high**
  - Background noise: **high**
  - First seen: **2024-03-02T06:45:00+00:00**
  - Last seen: **2024-07-29T16:15:00+00:00**
  - Link: **https://app.crowdsec.net/cti/185.191.126.213** lookup "app.crowdsec.net" Add URL
  - Targeted vulnerabilities: **CVE-2023-1389**
  - Aggressiveness (24h/7d/1m): **5/5/5**
  - Behavior:
    - **HTTP Exploit**
    - **SSH Bruteforce**
    - **HTTP DoS**
    - **HTTP Scan**
    - **VCS Bruteforce**
    - **HTTP Bruteforce**
    - **HTTP Crawl**
    - **Exploitation attempt**
  - Attacking details:
    - **TP-Link Archer AX21 - RCE**
    - **SSH Slow Bruteforce**
    - **HTTP DOS with invalid HTTP version**
    - **Nginx request limit exceeded**
    - **Bad User Agent**
    - **Gitea Bruteforce**
    - **SSH User Enumeration**
    - **HTTP Open Proxy Probing**
    - **HTTP Bruteforce**
    - **SSH Bruteforce**
    - **Endlessh Bruteforce**
    - **Aggressive Crawl**
    - **HTTP Probing**
    - **TP-Link Archer AX21 - RCE**
    - **SSH Slow User Enumeration**
    - **Suricata Severity 1 Event**
  - ATT&CK IDs:

- Detections, last: **1722234763**
  - IPsum: **Malicious**
  - VIPRE: **Malicious**
  - G-Data: **Malicious**
  - Lionic: **Malicious**
  - Certego: **Malicious**
  - CyRadar: **Malicious**
  - Fortinet: **Malicious**
  - SOCRadar: **Suspicious**
  - Antiy-AVL: **Malicious**
  - CINS Army: **Malicious**
  - BitDefender: **Malicious**
  - Criminal IP: **Malicious**
  - Juniper Networks: **Malicious**
  - ArcSight Threat Intelligence: **Suspicious**
- AbuseIPDB Report, retrieved at: **2024-07-30T10:34:16.570838Z**
  - ISP: **Amarutu Technology Ltd.**
  - UsageType: **Data Center/Web Hosting/Transit**
  - Country: **Netherlands (Kingdom of the)**
  - TOR: **False**
  - LastReported: **2024-07-30T10:32:16+00:00**
  - abuseConfidenceScore: **100**
  - Link: **https://www.abuseipdb.com/check/185.191.126.213** lookup "www.abuseipdb.com" Add URL
- AlienVault OTX pulses, by : **2024-07-30T10:34:16.681702Z**
  - Pulse Name: **SSH Brute-Force Honeypot Live**
    - Link: **https://otx.alienvault.com/pulse/60ece5998a5b54a5ffe75cb4** lookup "otx.alienvault.com" Add URL
    - Description: **every host is banned for 3 hours and receives an abuse report from me every 96 hours if it c**
    - Created: **2021-07-13T01:00:09.665000**
    - Tags: **Bruteforce, Brute-Force, SSH, Honeypot**
  - Pulse Name: **ETIC Cybersecurity 2024-07-30 Port Scan**
    - Link: **https://otx.alienvault.com/pulse/66a8151da14ba118368cceb2** lookup "otx.alienvault.com" Add URL
    - Created: **2024-07-29T22:18:05.915000**
  - Pulse Name: **TCP active portscan**
    - Link: **https://otx.alienvault.com/pulse/66794486bda6c3cf8823c604** lookup "otx.alienvault.com" Add URL
    - Description: **This pulse contains hourly updated list of detected scanning hosts performing active portsc**
    - Created: **2024-06-24T10:03:50.698000**
    - Tags: **portscan**
    - Targeted sectors: **Telecommunications**
  - Pulse Name: **Webscanners 2018-02-09 thru current day**
    - Link: **https://otx.alienvault.com/pulse/5a7e3e70c44e7b48947593a7** lookup "otx.alienvault.com" Add URL
    - Description: **Automated detection of webscanners based on 404**
    - Created: **2018-02-10T00:36:00.396000**
    - Tags: **webscanner, bruteforce, web app attack, probing, webscan, scanning**
    - Targeted sectors: **Finance**
  - Pulse Name: **Threat Listed**
    - Link: **https://otx.alienvault.com/pulse/666a51d286b205578ac80d48** lookup "otx.alienvault.com" Add URL
    - Created: **2024-06-13T01:56:34.275000**

Pasiruošę darbui ! ?

1. MISP
2. Shuffle
3. Elastic Search
4. RTIR
5. IntelOwl

Gerinimas ir Derinimas: inžinierinis procesas

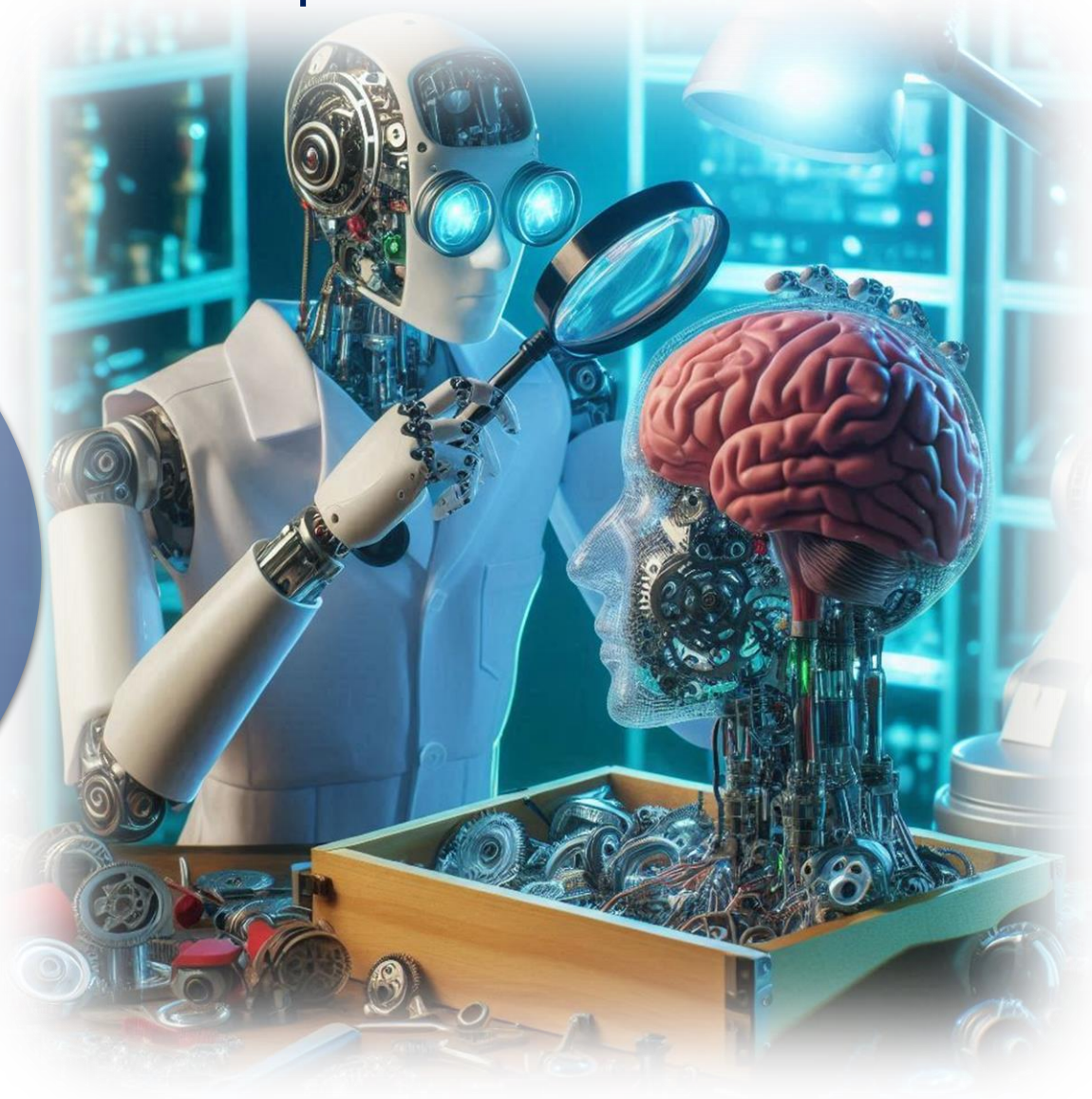
Derinti
- MISP užklausas
- ElasticSearch užklausas

+

Mažinti
- False positives
- False negatives

→

Varžteliai/sraigteliai
- Užklausos Shuffle sistemoje
- MISP Warninglists
- Filtrai
  - Blacklists
  - Whitelists



Apibendrinkime

Globalios pastangos

CSIRT bendruomenė betarpiškai dalinasi svarbia informacija ir tai suteikia reikšmingą pagalbą identifikuojant grėsmes

Jungiami taškai

API inžinerija, programinio kodo inžinerija apjungia komponentus į vieną sklandžiai dirbantį sprendimą

Lankstumas

Galimybė prieiti prie programinio kodo suteikia galimybę pritaikyti įrankius specifiniams poreikiams

NRD Cyber Security

Pabaiga