



**SECURITY
DAYS**

SAUGUMO OPERACIJŲ AUTOMATIZAVIMAS: NUO IDĖJOS IKI ĮRANKIO

Marius Urkis - NRD Cyber Security
CSIRT/SOC architektas

Rugsėjo 5 d. 2024

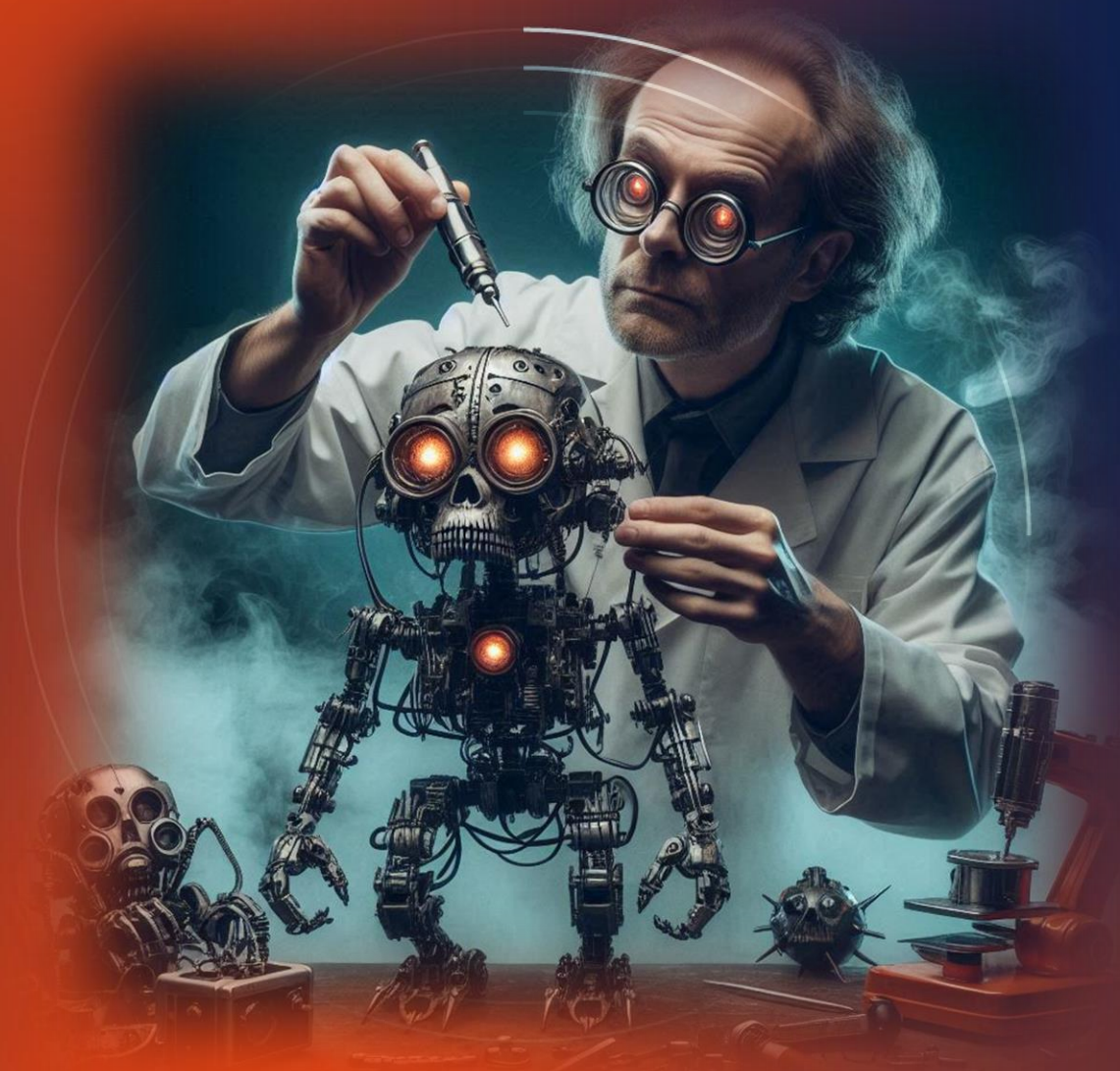
KIBERNETINIO SAUGUMO KONFERENCIJA

esd.eset.lt

Threat Hunting

Saugumo operacijų
automatizavimas: nuo idėjos
iki įrankio

Marius Urkis
mu@nrdcs.lt





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.

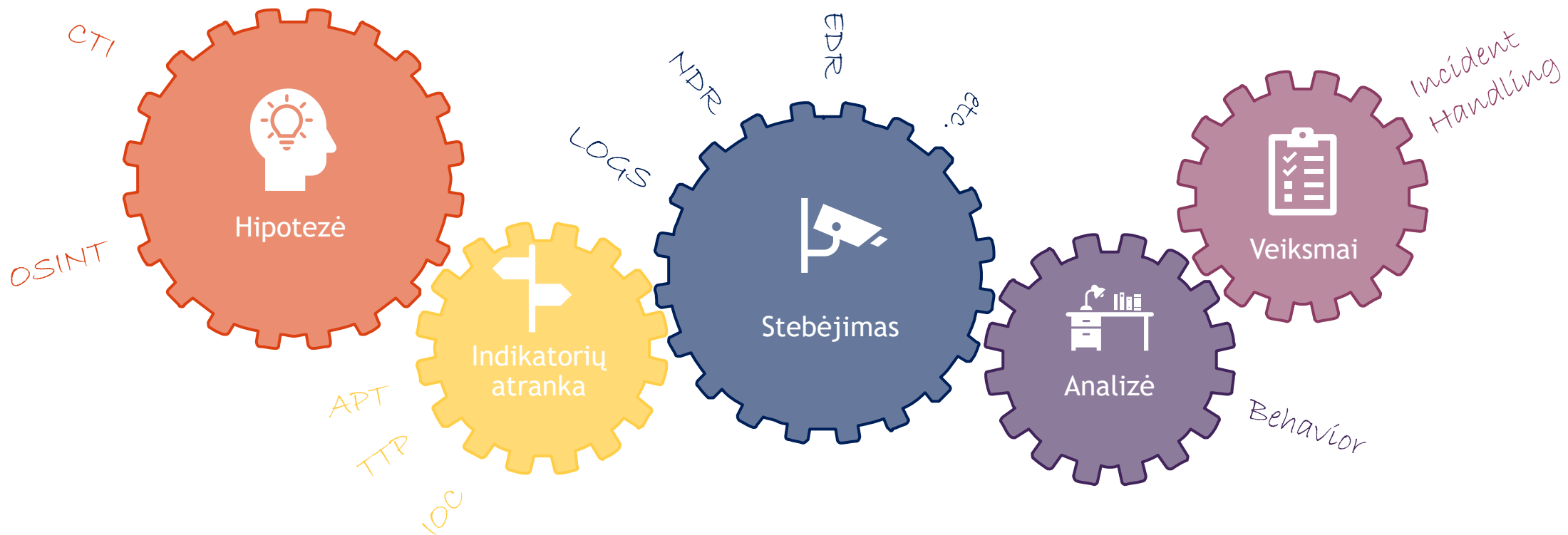
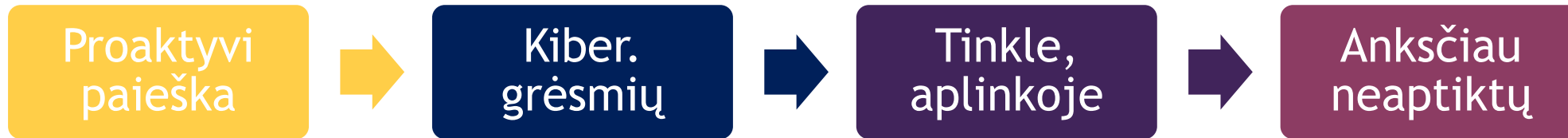
Specializacija

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

Sertifikatai

Sertifikuotas SIM3 auditorius | Sertifikuotas SOC-CMM vertintojas

Kas yra grėsmių medžioklė?



cert.gov.ua/article/6280129

gov.ua
Державні сайти України
Команда функціонує в складі Держспецзв'язку
CERT-UA
Computer Emergency Response Team of Ukraine

Люди із порушенням зору

Про CERT-UA | Новини | Рекомендації | З'яжіться з нами | Контакти

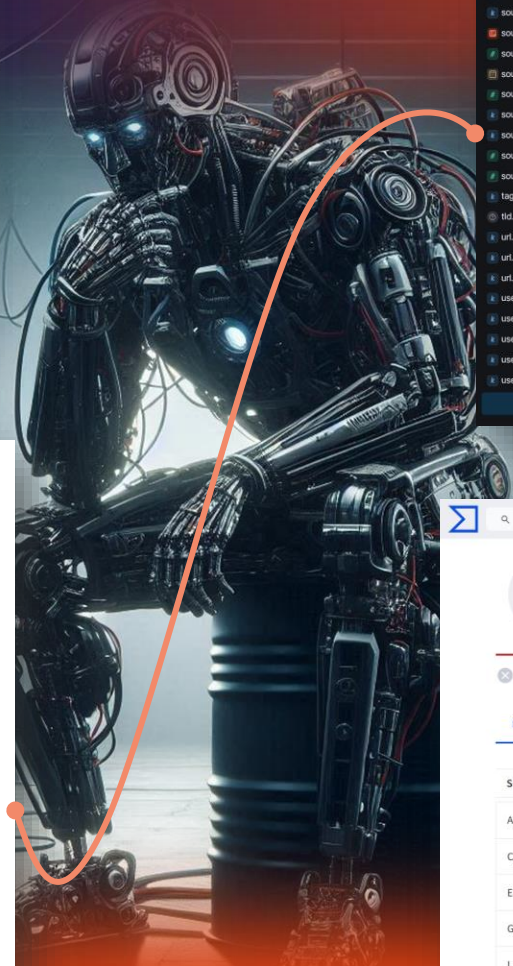
Головна | Новини | UAC-0063 атакує науково-дослідні установи України: HATVIBE + CHERRYSPY + CVE-2024-23692 (CERT-UA#10356)

21.07.2024

Загальна інформація
Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA досліджено кібератаку угруповання UAC-0063, здійснену 08.07.2024 по відношенню до однієї з українських науково-дослідних установ з використанням шкідливих програм HATVIBE та CHERRYSPY.
На етапі первинного ураження зловмисник, маючи доступ до облікового запису електронної пошти співробітника установи, здійснив відправку копії нещодавно відправленого листа десяткам адресатів (включаючи самого відправника), замінивши оригінальний документ-

За темою «ШПЗ»
24.07.2024
Точковий сплеск активності UAC-0057 (CERT-UA#10340)
17.07.2024
Ціліві кібератаки UAC-0180 у відношенні

Kaip tai galėtų veikti?



elastic

Find apps, content, and more.

Options New Open Share Alerts Inspect Save

Last 30 days Refresh

destination.ip: 208.197.3.8 x

Search field names

Filter by type

- source.domain
- source.domain_firstseen
- source.domain_prefix
- source.hostname
- source.ip
- source.ip.bytes
- source.ip_firstseen
- source.ip_firstseen_age
- source.label
- source.network
- source.packets
- source.port
- tags
- tid.domain
- url.hostname
- url.original
- url.path
- user_agent.device.name
- user_agent.name
- user_agent.original
- user_agent.os.full
- user_agent.os.name

12,898 hits

Jul 3, 2024 @ 14:25:59.518 - Aug 2, 2024 @ 14:25:59.518 (interval: Auto - 12 hours)

Documents Field statistics META

1 field sorted

Document

Aug 1, 2024 @ 28:28:51.548 @timestamp | Aug 1, 2024 @ 28:28:51.548 @version | 1 @destination.bytes | @destination.domain | windowupdate.com @destination.domain | Jul 17, 2024 @ 03:18:53.000 @destination.domain_firstseen_age | 392 @destination.domain_prefix | 9.au.download @destination.domain_prefix | 18149 @destination.geo.city.name | Phoenix @destination.geo.continent_name | NA @destination.geo.country_iso.code | US @destination.geo.location | Phoenix

Aug 1, 2024 @ 28:28:51.489 @timestamp | Aug 1, 2024 @ 28:28:51.489 @version | 1 @create.hive.case | Create Hive case | Create RTIR ticket | Create RTIR ticket | @destination.bytes | 0 @destination.domain | windowupdate.com @destination.domain | Jul 17, 2024 @ 03:18:53.000 @destination.domain_firstseen_age | 392 @destination.domain_prefix | 9.au.download @destination.domain_prefix | 18149 @destination.geo.city.name | Phoenix @destination.geo.continent_name | NA @destination.geo.country_iso.code | US @destination.geo.location | Phoenix

Aug 1, 2024 @ 28:28:51.489 @timestamp | Aug 1, 2024 @ 28:28:51.489 @version | 1 @destination.domain | windowupdate.com @destination.domain | Jul 17, 2024 @ 03:18:53.000 @destination.domain_firstseen_age | 392 @destination.domain_prefix | 9.au.download @destination.domain_prefix | 18149 @destination.geo.city.name | Phoenix @destination.geo.continent_name | NA @destination.geo.country_iso.code | US @destination.geo.location | Phoenix

Aug 1, 2024 @ 28:28:51.464 @timestamp | Aug 1, 2024 @ 28:28:51.464 @version | 1 @create.hive.case | Create Hive case | Create RTIR ticket | Create RTIR ticket | @destination.bytes | 0 @destination.domain | windowupdate.com @destination.domain | Jul 17, 2024 @ 03:18:53.000 @destination.domain_firstseen_age | 391 @destination.domain_prefix | 9.au.download @destination.domain_prefix | 18149 @destination.geo.city.name | Phoenix @destination.geo.continent_name | NA @destination.geo.country_iso.code | US @destination.geo.location | Phoenix

Aug 1, 2024 @ 28:28:51.462 @timestamp | Aug 1, 2024 @ 28:28:51.462 @version | 1 @destination.bytes | 0 @destination.domain | windowupdate.com @destination.domain | Jul 17, 2024 @ 03:18:53.000 @destination.domain_firstseen_age | 392 @destination.domain_prefix | 9.au.download @destination.domain_prefix | 18149 @destination.geo.city.name | Phoenix @destination.geo.continent_name | NA @destination.geo.country_iso.code | US @destination.geo.location | Phoenix

Aug 1, 2024 @ 28:28:51.429 @timestamp | Aug 1, 2024 @ 28:28:51.429 @version | 1 @create.hive.case | Create Hive case | Create RTIR ticket | Create RTIR ticket | @destination.bytes | 0 @destination.domain | windowupdate.com @destination.domain | Jul 17, 2024 @ 03:18:53.000 @destination.domain_firstseen_age | 391 @destination.domain_prefix | 9.au.download @destination.domain_prefix | 18149 @destination.geo.city.name | Phoenix @destination.geo.continent_name | NA @destination.geo.country_iso.code | US @destination.geo.location | Phoenix

Aug 1, 2024 @ 28:28:51.428 @timestamp | Aug 1, 2024 @ 28:28:51.428 @version | 1 @create.hive.case | Create Hive case | Create RTIR ticket | Create RTIR ticket | @destination.bytes | 1103106 @destination.domain | windowupdate.com @destination.domain | Jul 17, 2024 @ 03:18:53.000 @destination.domain_firstseen_age | 392 @destination.domain_prefix | 9.au.download @destination.domain_prefix | 18149 @destination.geo.city.name | Phoenix @destination.geo.continent_name | NA @destination.geo.country_iso.code | US @destination.geo.location | Phoenix

Rows per page: 100

Індикатори кіберзагроз

Файли:

```
197e86b76a41f154b64e092f7c3b306 6c439e62fb404e9095392878ef32f2fce18ce6155a1510f400540924
81cdcd59c86f8aa63810e4a085d673 f9baa77117f5a058461e859efc67c8e1ac205d1536326e01a030ab
7a2a8c002a5e22c6231885e1ccf82bd1 593ca06d639f7c3e99db768b318b765e7585496debfd553cd1df03f
7f865b65a82dcb18385644e0fd894727 259619899c60aa46df4f83558606813c79927c141bbf4b21bbf07b2
33c3e4599ad678133905e6c1589c12d2 e6daa00e095948acfc176d71c5bf667a0403e5259653ea5ac8950ae
d618720afd0ee49601f7933c414ffbb5 bcdbe035001af9d2cc173e975fa0b13b133e613b7d9b6e90df86672
8e1b29046c7f5bd1ddd4f549e255592 f4ada2b858c84da8b53c08ce4579f8b5b5df25e0d0f17ee0b48e10c
d84043b72dbced92b2d60c2725bd674f 93322be078555e6e27d2b09832c18e39c115e6a6fbff64b1e590e1d
34ced721349626ce81c11693b9243c19 a171e9c413518750806ae094e32f15791d4193229c598642760af5
d0c3b49e788600ff3967f784eb5de973 332d9db35daa83c5ad226b9b5f50e992713bc6a69c9ecd52a1223b81
8159abd281783e0ae601afce3b7d23b1 48a30083f115ca0d359afc175cf942367207a73fdda28778e2b2645
```

Мережеві:

```
hXp://trust-certificate[.]net/setup.php
hXp://trust-certificate[.]net/tmp/379.zip
hXPs://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
hXp://45.136.198[.]184/connect.php
hXp://45.136.198[.]184/input.php
hXp://45.136.198[.]184/output.php
hXp://5.45.70[.]178/RemoteAssistanceSvc.htm
```

exchange.dumb1.com

13 / 93

13/93 security vendors flagged this domain as malicious

exchange.dumb1.com Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Creation Date: 24 years ago Last Analysis Date: 2 hours ago

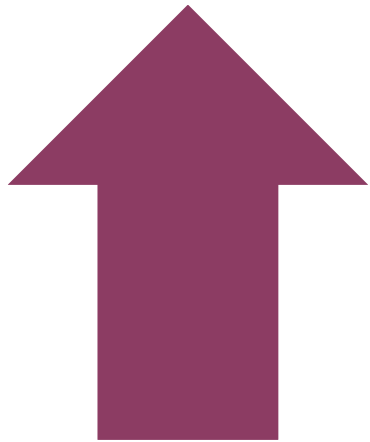
Community Score: Malicious, Phishing, command and control, top-1M

DETECTION DETAILS RELATIONS COMMUNITY 10

Security vendors' analysis

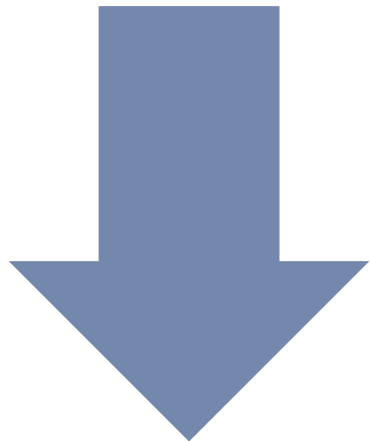
Vendor	Analysis	Vendor	Analysis
Anty-AVL	Malicious	BitDefender	Phishing
CyRadar	Malicious	Emsisoft	Phishing
ESET	Phishing	Fortinet	Phishing
G-Data	Phishing	Kaspersky	Malware
Lionic	Malicious	Netcraft	Malicious
Seclookup	Malicious	Sophos	Malicious
VIPRE	Malware	AlphaSOC	Suspicious
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AllLabs (MONITORAPP)	Clean

Mūsų įrankiai: atviras kodas



Privalumai

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



Trūkumai

- Reikalingos žinios
- Aptarnavimo stoka



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



Rankis:

- MISP, Malware Information Sharing Platform
- <https://github.com/MISP/MISP>

CTI valdymo priemonė

Sukurtas dalinimuisi

Kibernetinių grėsmių duomenys bei kontekstas

Bendruomenės pajėgumai



REST API

- <https://www.misp-project.org/openapi/>

FIN-7 APT activity

Event ID: 1752
 UUID: c925b53f-3d4d-4656-aa12-c9b8b4e39b2
 Creator org: NRDCS
 Owner org: NRDCS
 Creator user: mu@nrds.lt
 Protected Event (experimental): Event is in unprotected mode.
 Tags: APT, X, +, +
 Date: 2024-07-15
 Threat Level: 7 Undefined
 Analysis: Completed
 Distribution: All communities
 Published: last published at 2024-08-01 16:12:37
 Attributes: 108 (3 Objects)
 First recorded change: 2024-07-15 16:09:23
 Last change: 2024-08-01 15:37:22
 Modification map: 0 (0) - restricted to own organisation only

Related Events

Warning: Potential false positives (show)
 Specialized list of vpn-ipv4 addresses belonging to common VPN providers and datacenters

Bendroji informacija

Koreliacija ir false-positive požymiai

FIN-7 APT activity

Event ID: 1752
 UUID: c925b53f-3d4d-4656-aa12-c9b8b4e39b2
 Creator org: NRDCS
 Owner org: NRDCS
 Creator user: mu@nrds.lt
 Protected Event (experimental): Event is in unprotected mode.
 Tags: APT, X, +, +
 Date: 2024-07-15

Related Events

Order by date

CE... Daily Incremental ThreatFox Import - 2024-05-03	8
MalwareBazaar malware samples for 2024-04-30	1
MalwareBazaar malware samples for 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

Date	Context	Category	Type	Value	Tags	Galaxies	Custom	Correlate	Related Events	Feed hits	IQ	Distribution	Sightings	Activity	Actions
2024-07-30	008...bat	Network activity	url	in.runtasticcenterbusiness								Inherit			
2024-07-15	0ae...338	Persistence mechanism	registry	VF@Program\Fac65472404-erba72a.exe & *PUBLIC%\Chest\0001.7z; c:\PUBLIC\N\Chest\q1234567890								Inherit			
2024-07-15	778...488	Payload delivery	filename	anyconnect.win.msi								Inherit			

Taksonomija, kontekstas

1752: FIN-7 APT ac...

Galaxies

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

Indikatoriai

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:

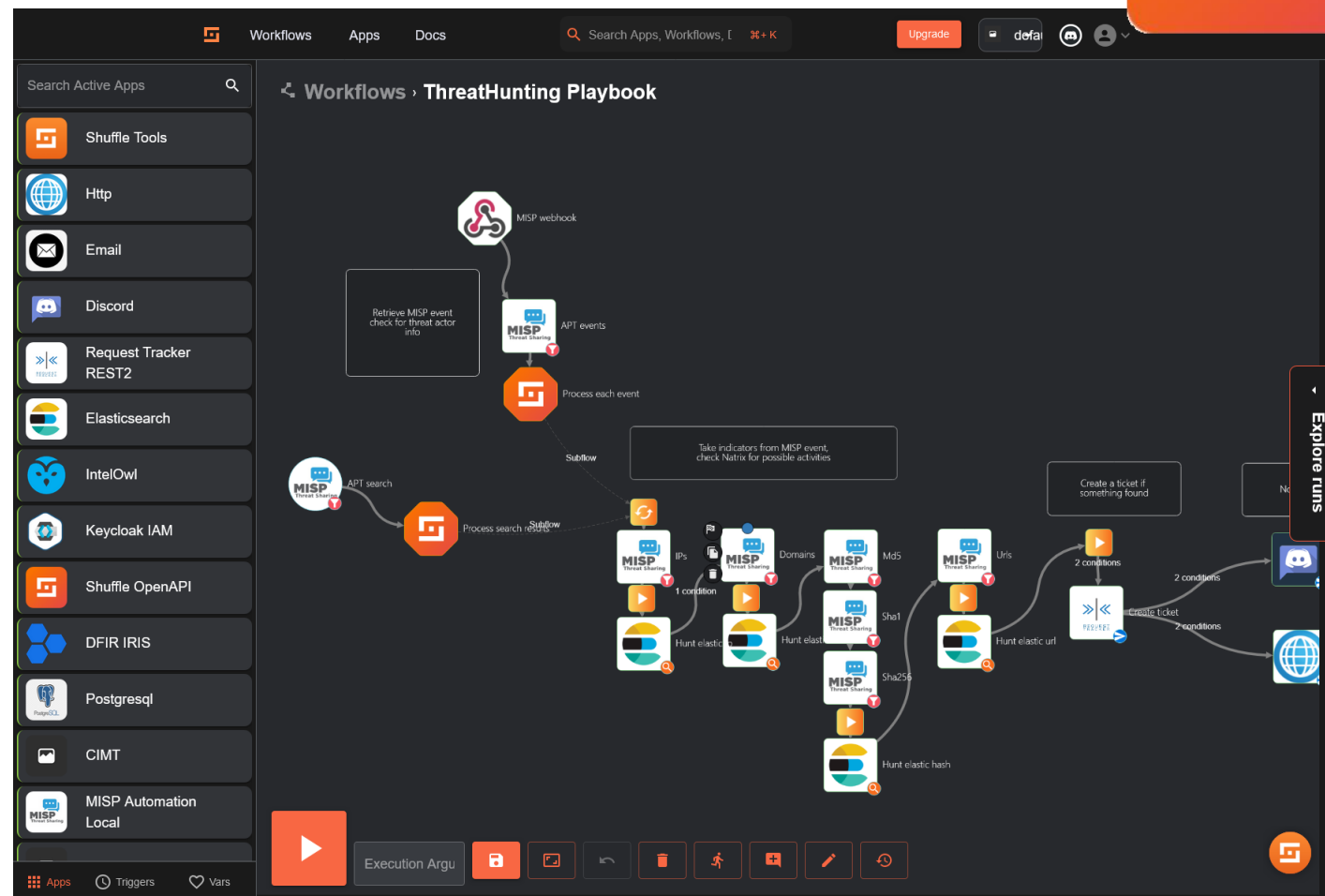
- Shuffle, atviro kodo SOAR
- <https://github.com/Shuffle/Shuffle>

Apjungia

- Aplikacijas, sąlygas
- Į automatizuotas veiksmų sekas

Savybės

- Workflow dizaineris
- Sąlygos: laiko grafikas, webhook
- Aplikacijų kūrimas
- OpenAPI importavimas



Persiųsti MISP srautą į Shuffle apdorojimui

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 functi
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

CTI champion



```

1 {
2   "returnFormat": "json",
3   "uuid": "$exec.Event.uuid",
4   "tag": "misp-galaxy:threat-actor=%",
5   "last": "1d",
6   "limit": "10",
7   "published": true
8 }
    
```

Žingsnis 3: Peržiūrėti žurnalus



Paieška NDR įrašų istorijoje

- NDR - Network Detection and Response

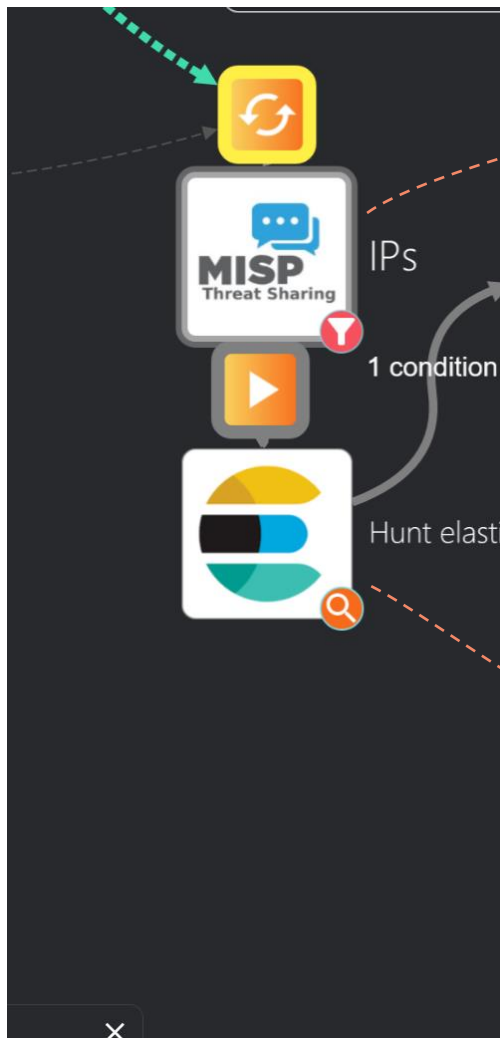
- ElasticSearch

- <https://www.elastic.co/guide/en/elasticsearch/reference/current/docs.html>

The screenshot shows the Elastic Search web interface. At the top, there's a search bar with the query '*:cs-nsm-*' and a filter 'destination.ip: 209.197.3.8'. The results show 12,898 hits. A histogram on the right shows the distribution of hits over time, with a peak around July 28th. Below the histogram, there's a 'Documents' tab showing a list of search results. Each result includes a timestamp, version, and various destination-related fields.

@timestamp	@version	destination.bytes	destination.domain	destination.firstseen
Aug 1, 2024 @ 20:28:51.540	1	0	windowsupdate.com	Jul 17, 2024 @ 03:18:53.000
Aug 1, 2024 @ 20:28:51.489	1	0	172.17.1.1	Jul 17, 2024 @ 03:18:53.000
Aug 1, 2024 @ 20:28:51.489	1	0	windowsupdate.com	Jul 17, 2024 @ 03:18:53.000
Aug 1, 2024 @ 20:28:51.464	1	0	windowsupdate.com	Jul 17, 2024 @ 03:18:53.000
Aug 1, 2024 @ 20:28:51.462	1	0	windowsupdate.com	Jul 17, 2024 @ 03:18:53.000
Aug 1, 2024 @ 20:28:51.429	1	0	windowsupdate.com	Jul 17, 2024 @ 03:18:53.000
Aug 1, 2024 @ 20:28:51.428	1	1103106	windowsupdate.com	Jul 17, 2024 @ 03:18:53.000

Automatizuojame: surinkti ir ieškoti



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

```

Filters Math Python + Autocomplete
1 {
2   "returnFormat": "json",
3   "type": "ip-dst",
4   "to_ids": true,
5   "enforceWarninglist": true,
6   "uuid": "$misp_event.uuid"
7 }
    
```

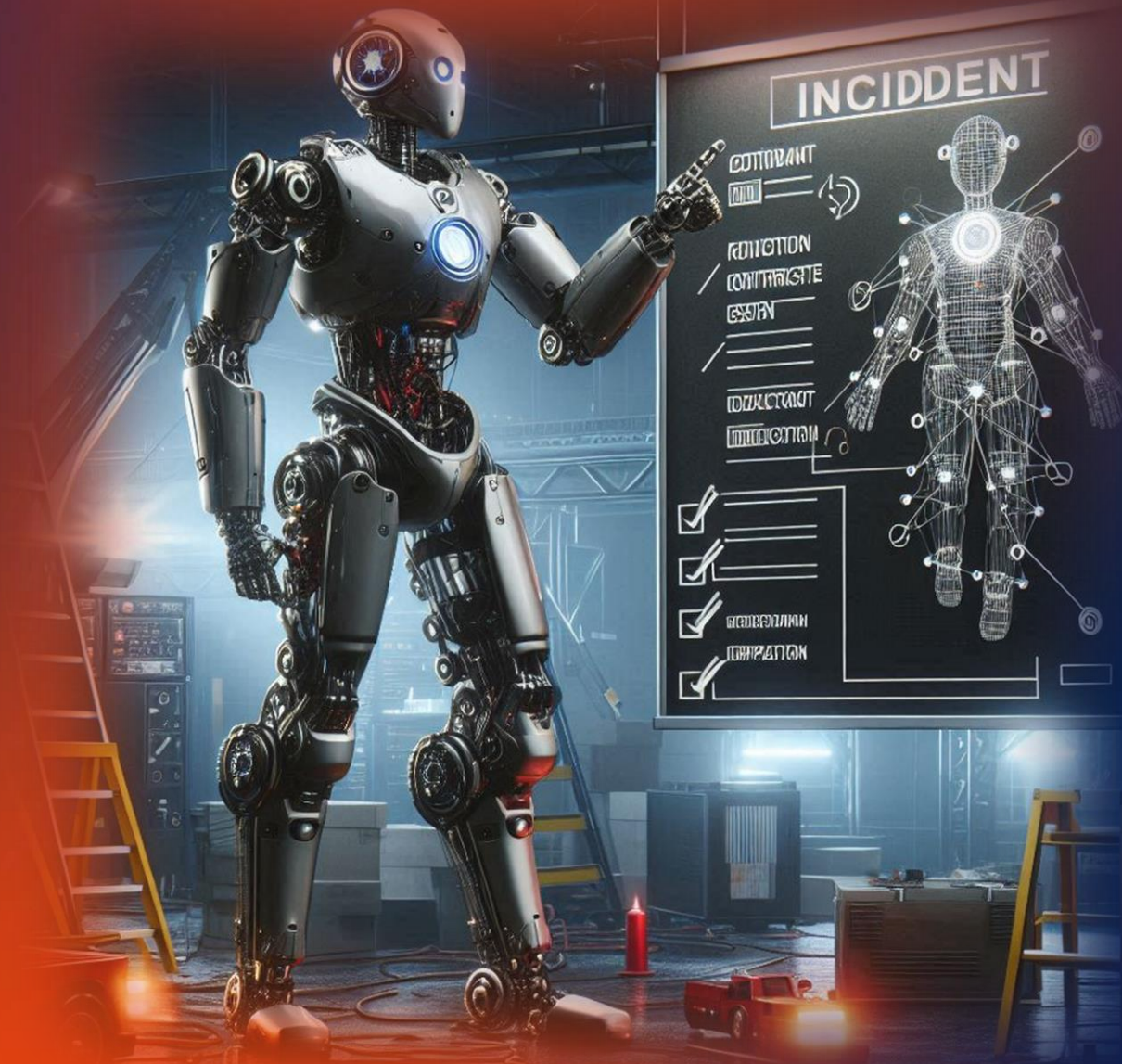
Ištraukti agreguotus ir filtruotus duomenis

```

Filters Math Python + Autocomplete
1 {
2   "aggs": {"0": {"terms": {"field": "observer.name", "order":
3     {"_count": "desc"}, "size": 3, "shard_size": 25},
4     "aggs": {"1": {"terms": {"field": "source.ip", "order": {"_count":
5       {"multi_terms": {"terms": [{"field": "destination.ip"}, {"field":
6         , "size": 5, "shard_size": 25}}}}}},
7     "sort": [{"@timestamp": {"order": "desc", "unmapped_type": "boolean"}
8     "size": 0,
9     "query": {"bool": $filter_ip.message
    }
  }
    
```

*History:
Last 60 days?*

Žingsnis 4: Registruoti incidentą



Registravimas: incidentai ir bilietų sistema

Rankis:

- Ticketing System
- Request Tracker for Incident Response
- <https://github.com/bestpractical/rt>
- <https://github.com/bestpractical/rtir>

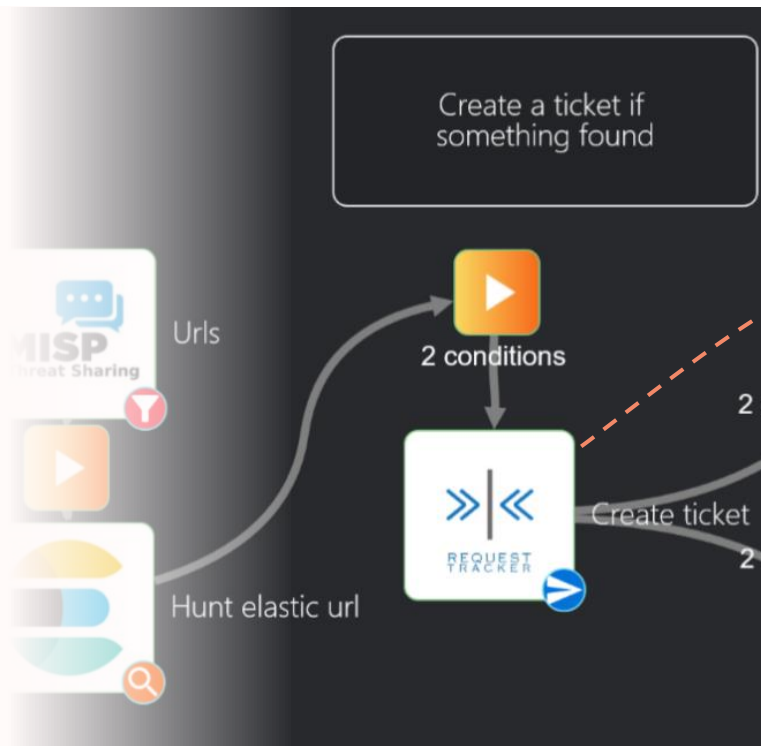
Sąvybės

- 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

The screenshot displays the Request Tracker (RT) web interface. At the top, there is a navigation bar with menus for Home, RTIR, Search, Reports, Articles, Tools, and a user profile for 'marius'. A search bar and a 'Create new ticket' button are also visible. The main content area is titled 'RTIR at a glance' and contains several panels:

- New unlinked Incident Reports...:** A table with columns for #, Subject, Requestor, Owner, Due, Queue, and Bulk Reject. One entry is shown: #223, 'Incident report from CIMT', requestor '<cybersec.customer@nrdfs.it>', owner 'marius (Marius Urkis)', due '4 hours', and queue 'Incident Reports'.
- Most due incidents owned by marius:** A table with columns for #, Subject, Due, Owner, Priority, and Updates. Three entries are shown: #188 (Event Rule description here From Matrix, 24 hours ago, Low priority, 2 updates), #209 (Phishing resource ootexa[.]com, 119 minutes, Medium priority, 4 updates), and #215 (Ongoing ITG05 operations leverage evolving malware arsenal in global campaigns, 48 hours, Low priority, 8 updates).
- Most due unowned incidents:** A table with columns for #, Subject, Due, Owner, Priority, and Updates. One entry is shown: #289 (Automatic Threat Hunting findings, Nobody in particular, Low priority, 1 update).
- Work with constituency:** A section for managing constituencies.
- Queue list:** A summary table showing counts for Countermeasures, Incident Reports, Incidents, and Investigations across different states like pending activation, active, and pending removal.
- Refresh:** A button to refresh the page.

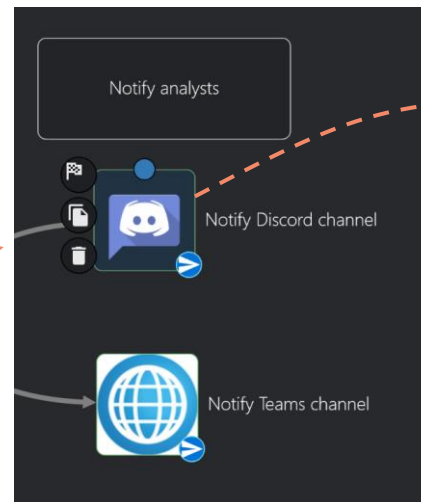
„Ticketing“ automatizavimas



Registruoti incidentą sistemoje

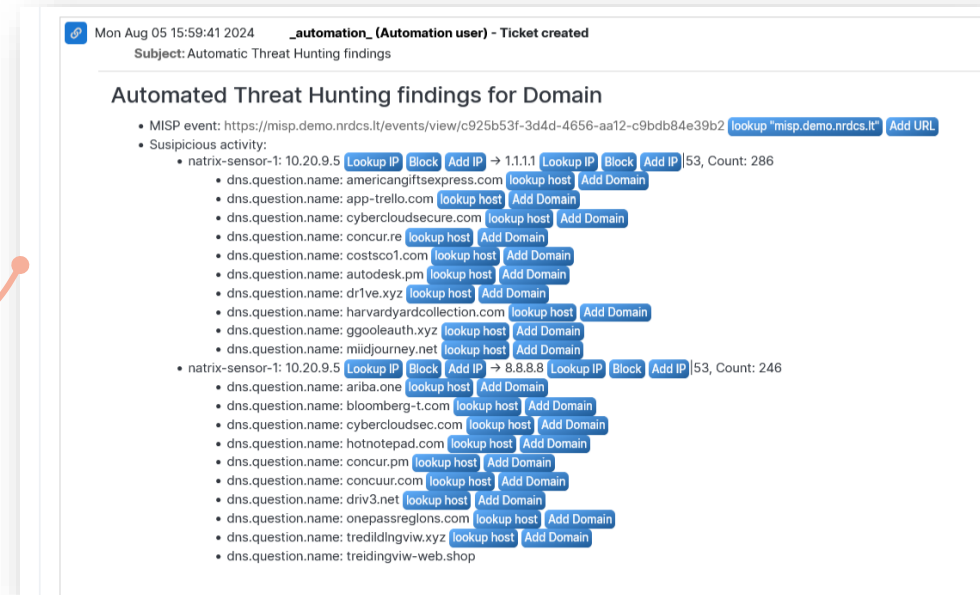
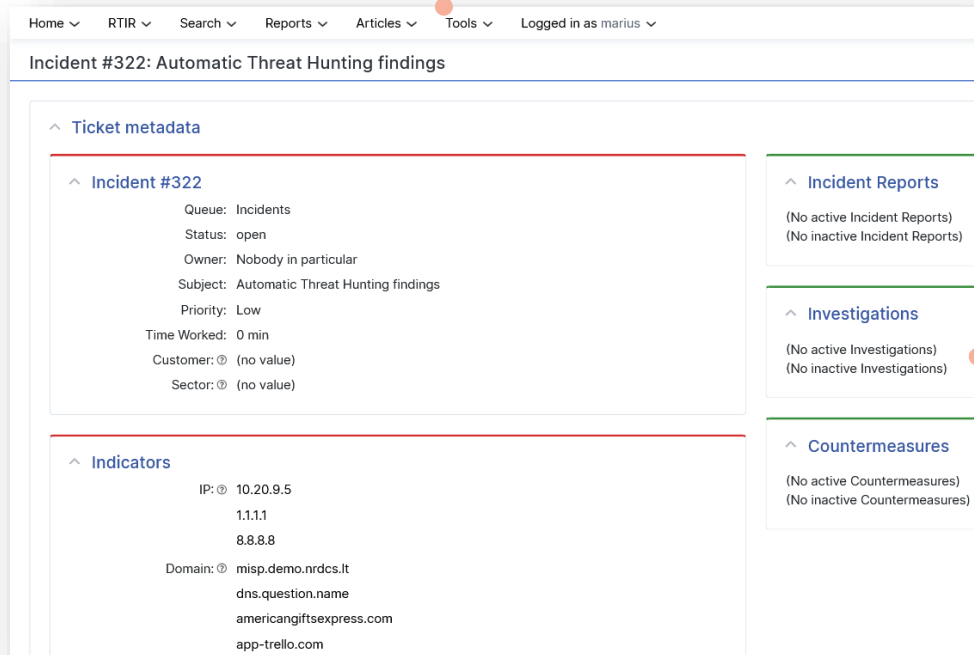
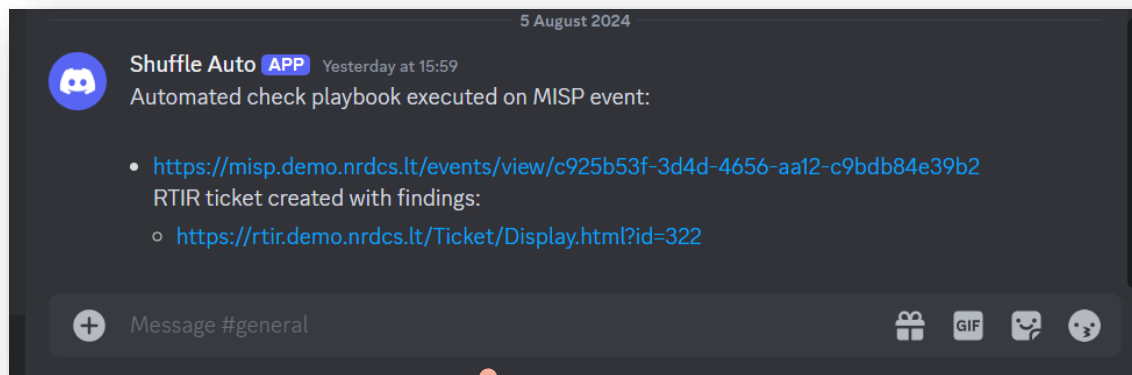
```
Filters Math Python + Autocomplete
1 {
2   "Queue": "$rtir_queue",
3   "Subject": "Automatic Threat Hunting findings",
4   "Content": "$formatted_output.message",
5   "ContentType": "text/html"
6 }
```

Informuoti analitikus - Discord, Teams, t.t.



```
Filters Math Python + Autocomplete
1 Automated check playbook executed on MISP event:\n
2 - $MISP_BASEURL/events/view/$misp_event.uuid \n
3 RTIR ticket created with findings:\n
4 - https://rtir.demo.nrdcs.lt/Ticket/Display.html?id=$create_ticket.body.id
```

Rezultatas



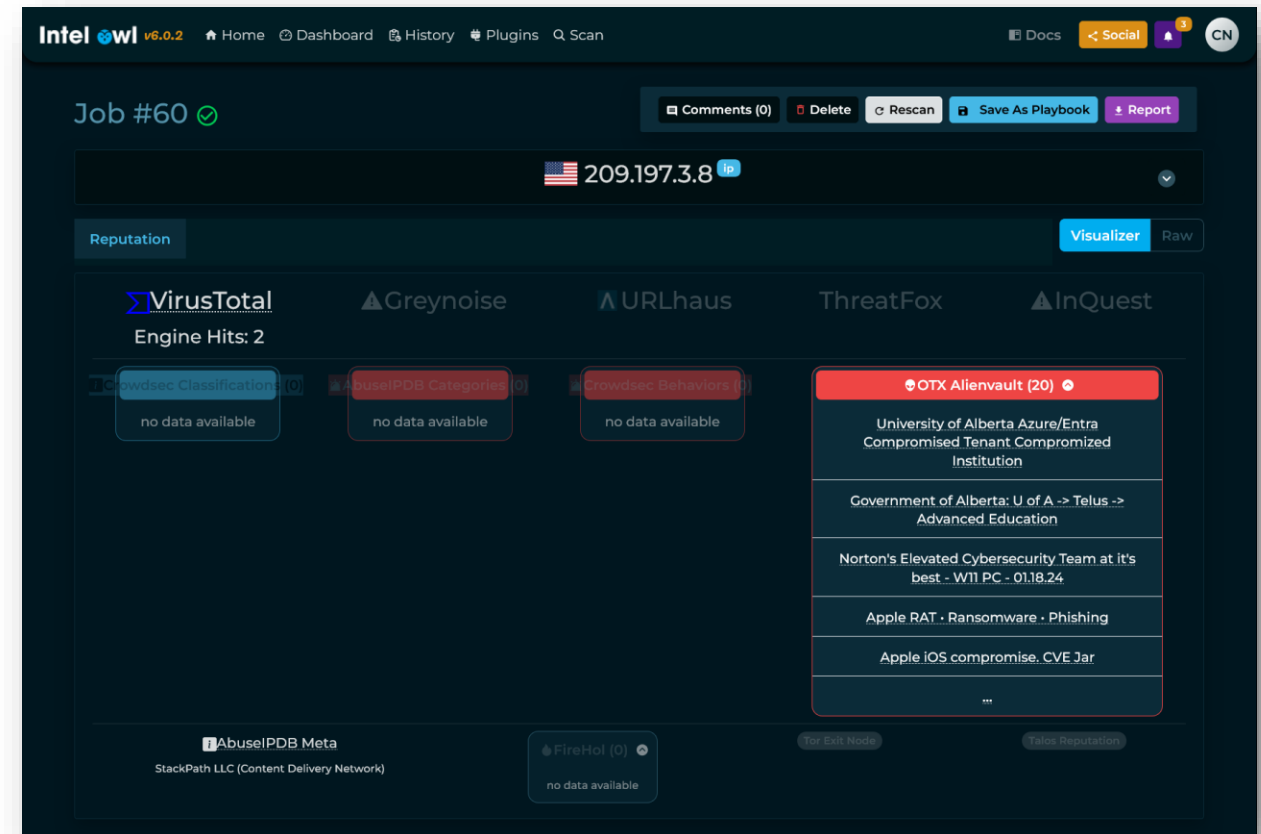
Žingsnis 5: Atlikti analizę



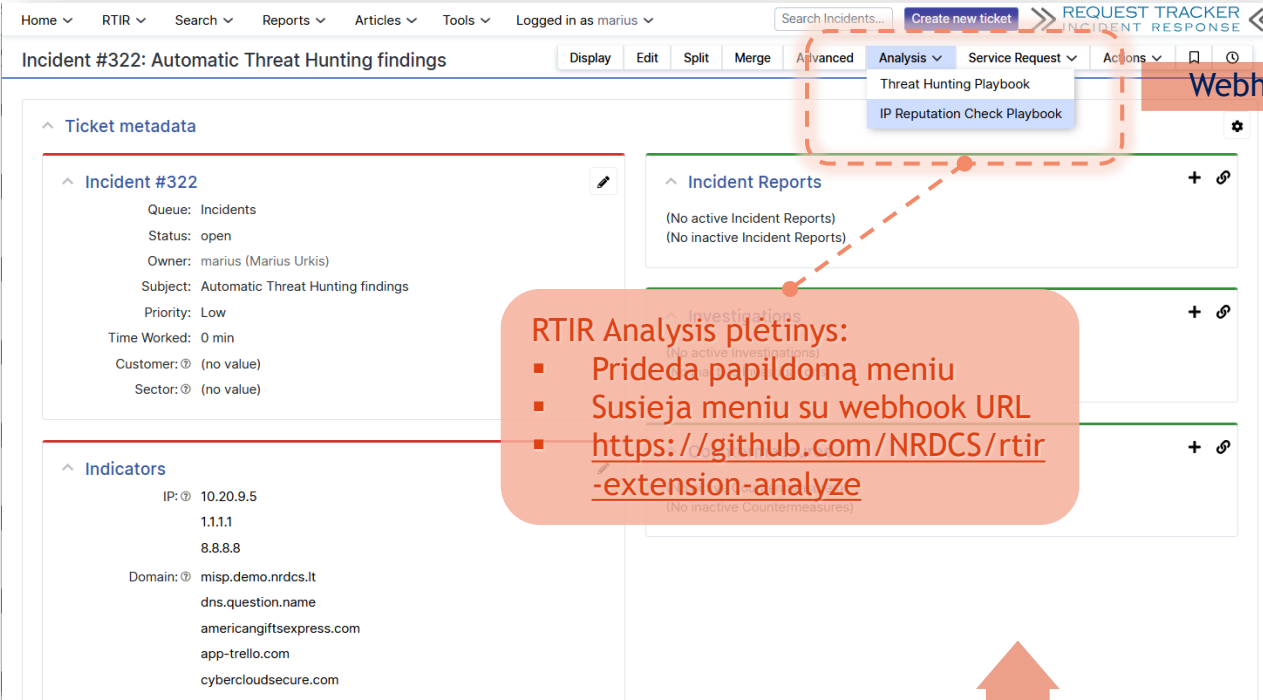
Analizė

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>



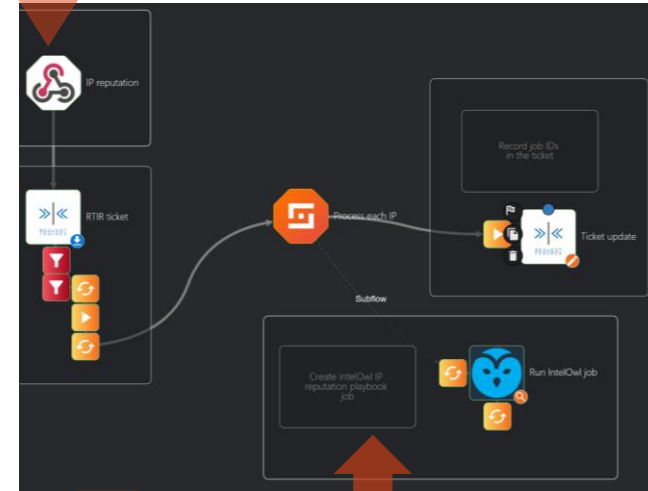
Pridėkim RTIR įrankiui analitines funkcijas



RTIR Analysis plėtinys:

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

Webhook kreipinys



Rezultatai pridunami prie incidento



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
 - Endless 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: Amaru 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



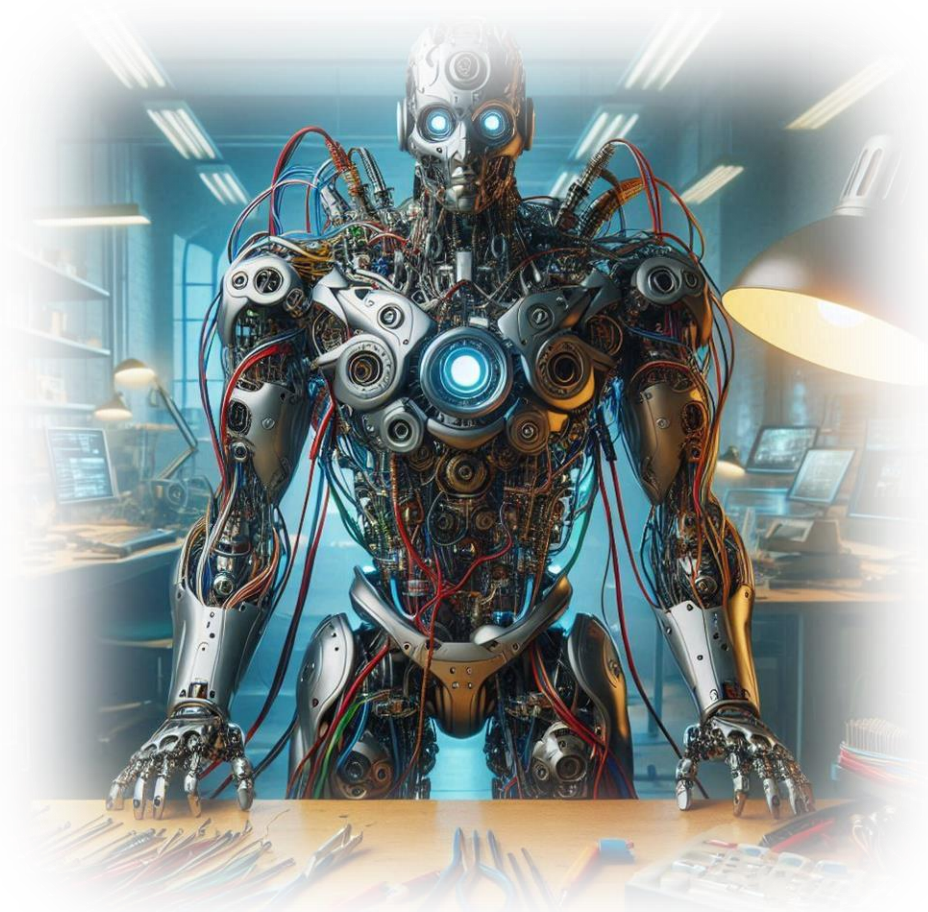
4

RTIR



5

IntelOwl



Gerinimas ir Derinimas: inžinierinis procesas

Derinti

- MISP užklausas
- ElasticSearch užklausas



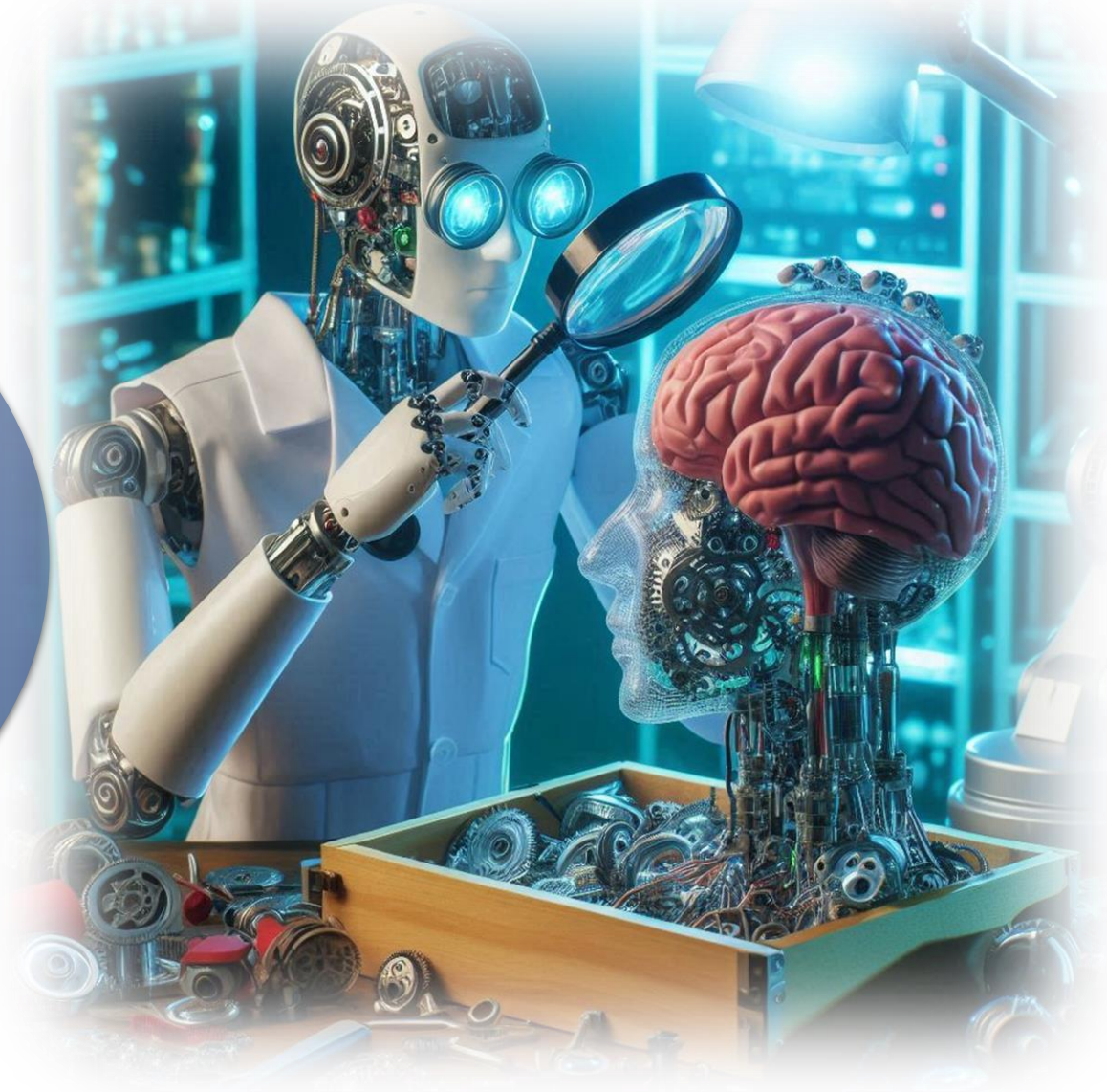
Mažinti

- False positives
- False negatives

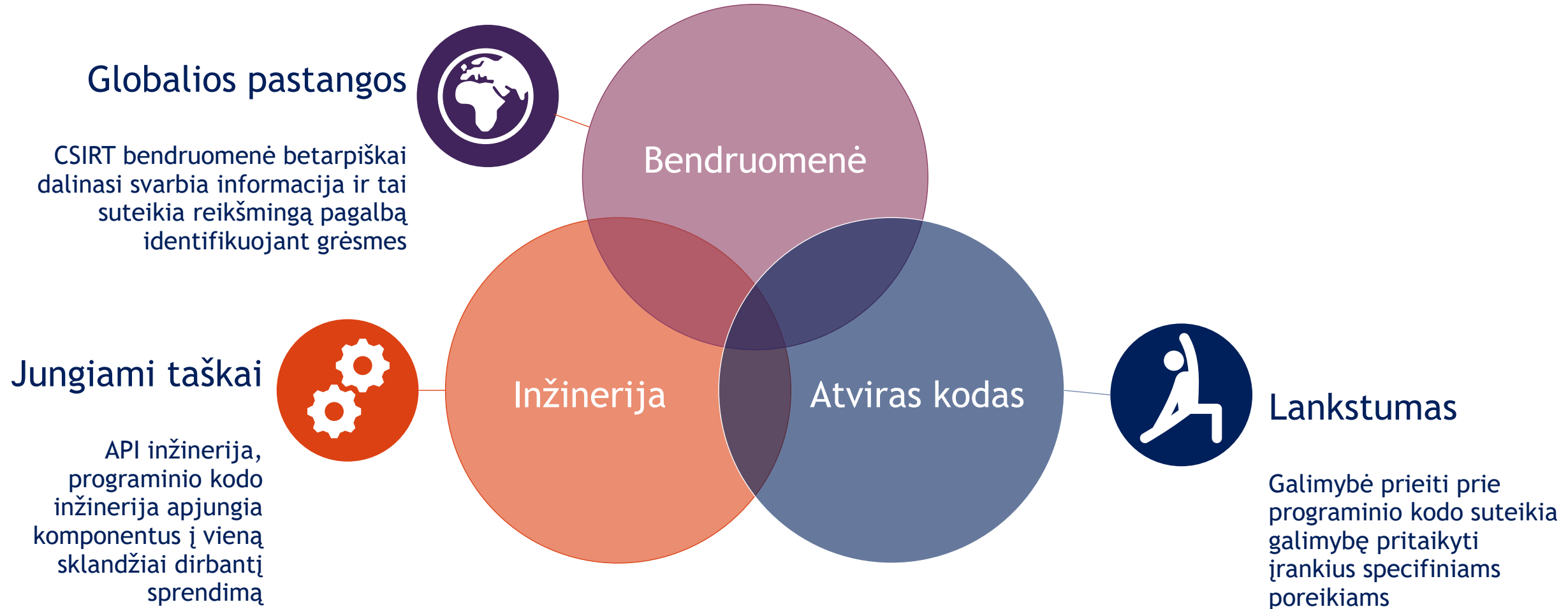


Varžteliai/sraigteliai

- Užklausos Shuffle sistemoje
- MISP Warninglists
- Filtrai
 - Blacklists
 - Whitelists



Apibendrinkime



Pabaiga

