



IntelOwl Project

making the life of cyber security analysts easier

HackInBo '23

\$ say hi to the team :)



Matteo Lodi Simone Berni

@matte_lodi



@0ssig3no

mlodic



Ossigeno

certego

Threat Intelligence Team

- Higher pay grades
- Fast career paths
- Never-ending learning jobs
- Challenging
- Ethical

FORTUNE | EDUCATION

ARTICLES CAREER GUIDES RANKINGS ▾ MORE ▾

ARTICLES » THE CYBERSECURITY INDUSTRY IS SHORT 3.4 MILLION WORKERS—THAT'S GOOD NEWS FOR CYBER WAGES

The cybersecurity industry is short 3.4 million workers —that's good news for cyber wages

BY SYDNEY LAKE

October 20, 2022, 3:01 PM

ref: [Fortune](#)

NEWS ITEM

Higher Education in Europe: Understanding the Cybersecurity Skills Gap in the EU

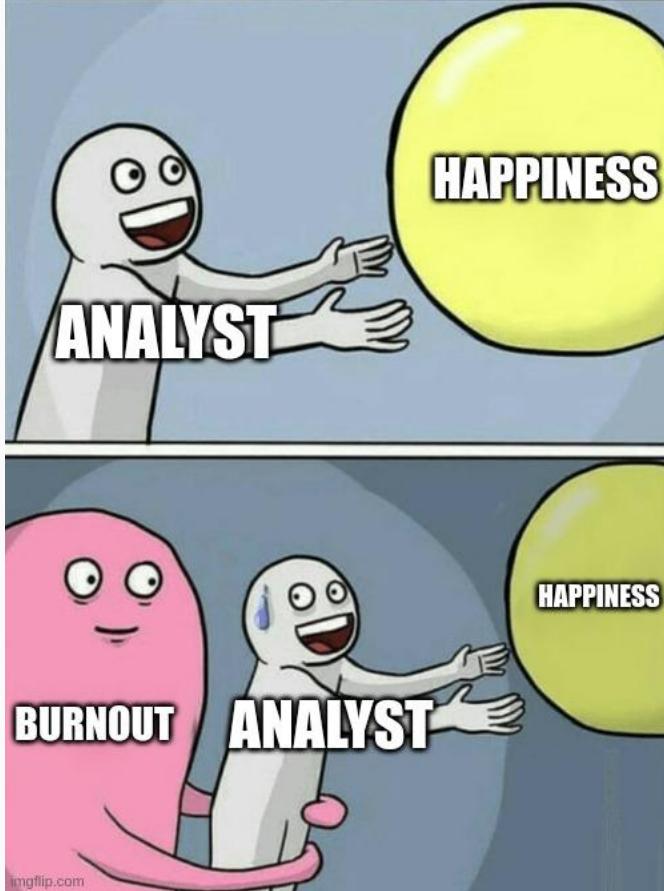
Cybersecurity graduates are expected to double in number in the next 2-3 years as shown by the Higher Education Database managed by European Union Agency for Cybersecurity.

Published on November 24, 2021

ref: [Enisa](#)

- Higher pay
- Fast career
- Never-endin
- Challenging
- Ethical





Cyber security analysts are:

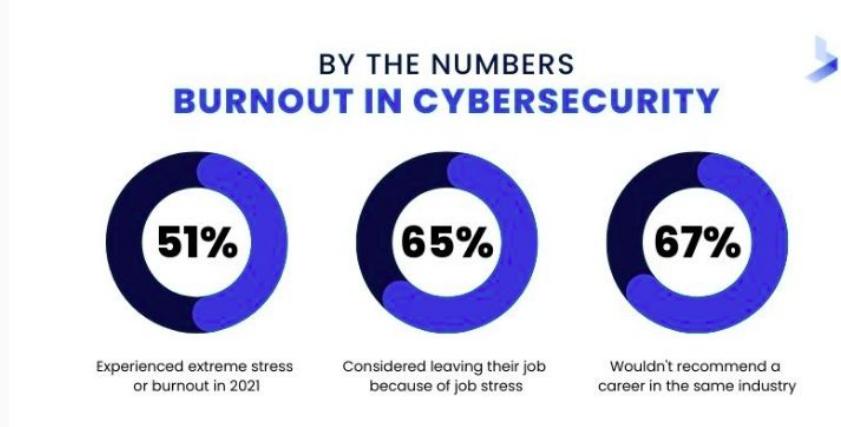
- understaffed
- overworked
- working 24/7
- without work-life balance
- used as scapegoats
- do a lot of manual work

which could be automated

Cybersecurity burnout is real. And it's going to be a problem for all of us

Burnout might be the most critical cybersecurity risk facing organizations in 2022. So, how do we tackle it?

ref: [ZDNet](#)



ref: [Bitlyft](#)

2017:

- Working in a little team of cyber security analysts
- Overwhelmed by security alerts
- Burnt-out myself

2017:

- Working in a little team of cyber security analysts
- Overwhelmed by security alerts
- Burnt-out myself

We needed to start to **automate** our most common workflows.



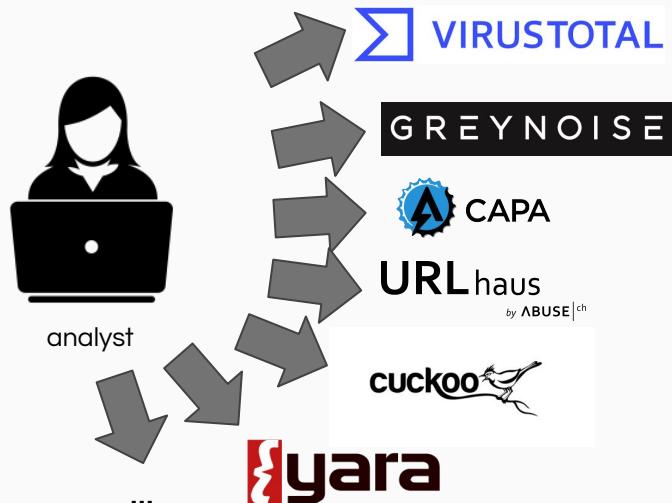
manual work

automation

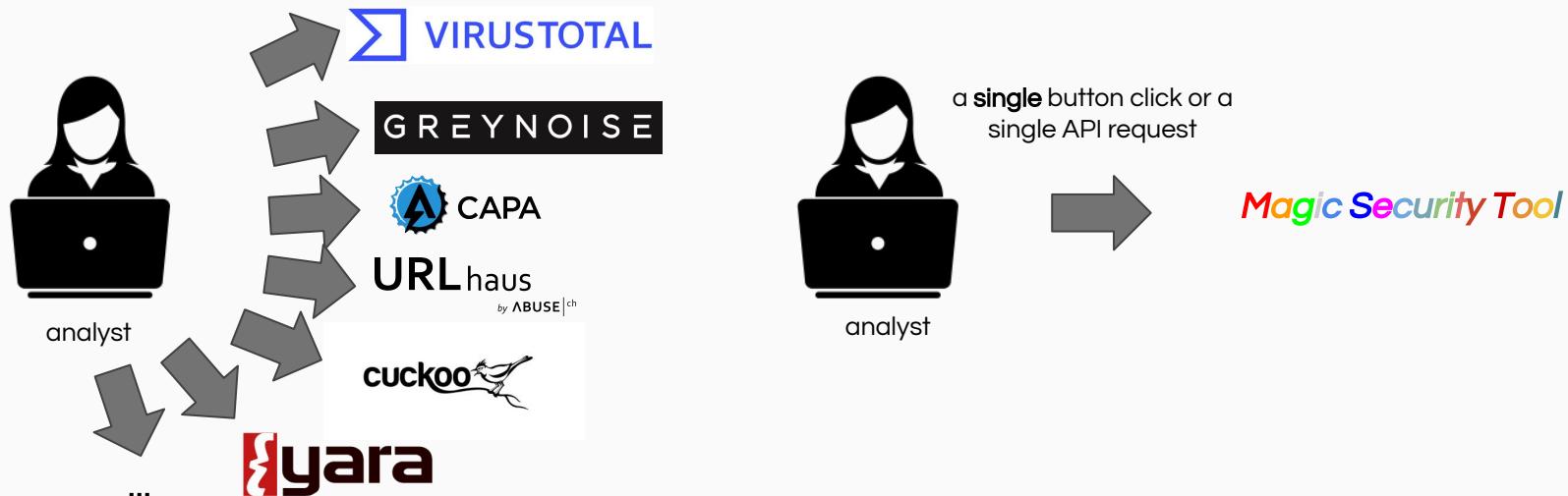
The bottleneck: acquisition of threat intelligence context



The bottleneck: acquisition of threat intelligence context



The bottleneck: acquisition of threat intelligence context



We were looking for a tool

Our requirements were:

We were looking for a tool

Our requirements were:

- Automated extraction of threat intelligence data from different sources
- Full-featured Web Application with user-friendly interface



We were looking for a tool

Our requirements were:

- Automated extraction of threat intelligence data from different sources
- Full-featured Web Application with user-friendly interface
- Client library for easy integrations with other security tools
- High possibility of customization to allow different use cases



We were looking for a tool

Our requirements were:

- Automated extraction of threat intelligence data from different sources
- Full-featured Web Application with user-friendly interface
- Client library for easy integrations with other security tools
- High possibility of customization to allow different use cases
- High level of scalability and speed
- Open source



We were looking for a tool

Our requirements were:

- Automated extraction of threat intelligence data from different sources
- Full-featured Web Application with user-friendly interface
- Client library for easy integrations with other security tools
- High possibility of customization to allow different use cases
- High level of scalability and speed
- Open source
- Written with the most recent technologies
- Well maintained and updated





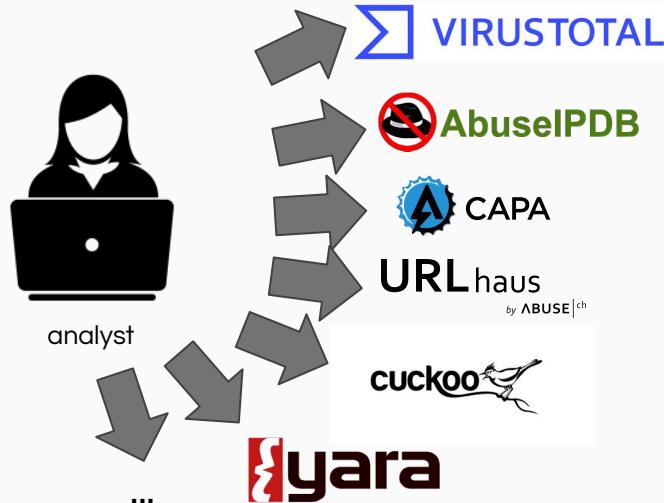
Intel owl

Born in Certego at the start of 2020, it is a great example of a successful Open Source project: right now it is one of the most popular Threat Intel projects on GitHub (>2.8k stars).

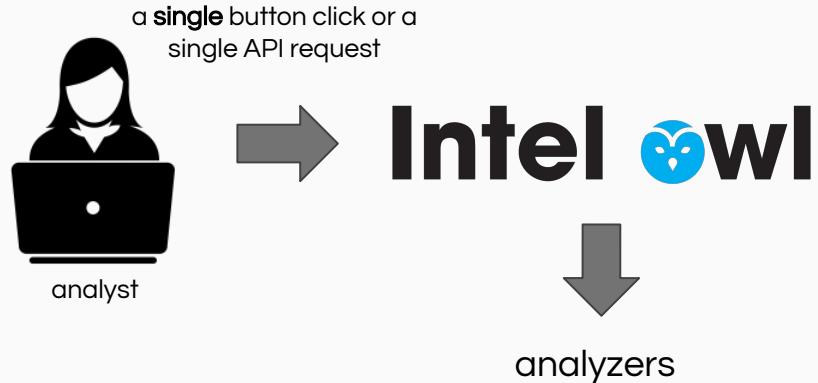
IntelOwl provides data **enrichment** of threat intel artifacts (IP, Domain, URL, files, PCAP, hash, etc).



WithOUT Intel Owl



With Intel Owl

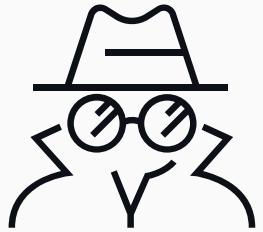


The screenshot shows the GitHub repository page for IntelOwl. It includes sections for Code, Issues (86), Pull requests (7), and Discussions. A prominent pull request from mlodic and dependabot[bot] is shown, merged last week with 1,251 approvals. The README.md file is also visible.

The most common (and open source) technologies and framework are used and we keep them constantly updated:

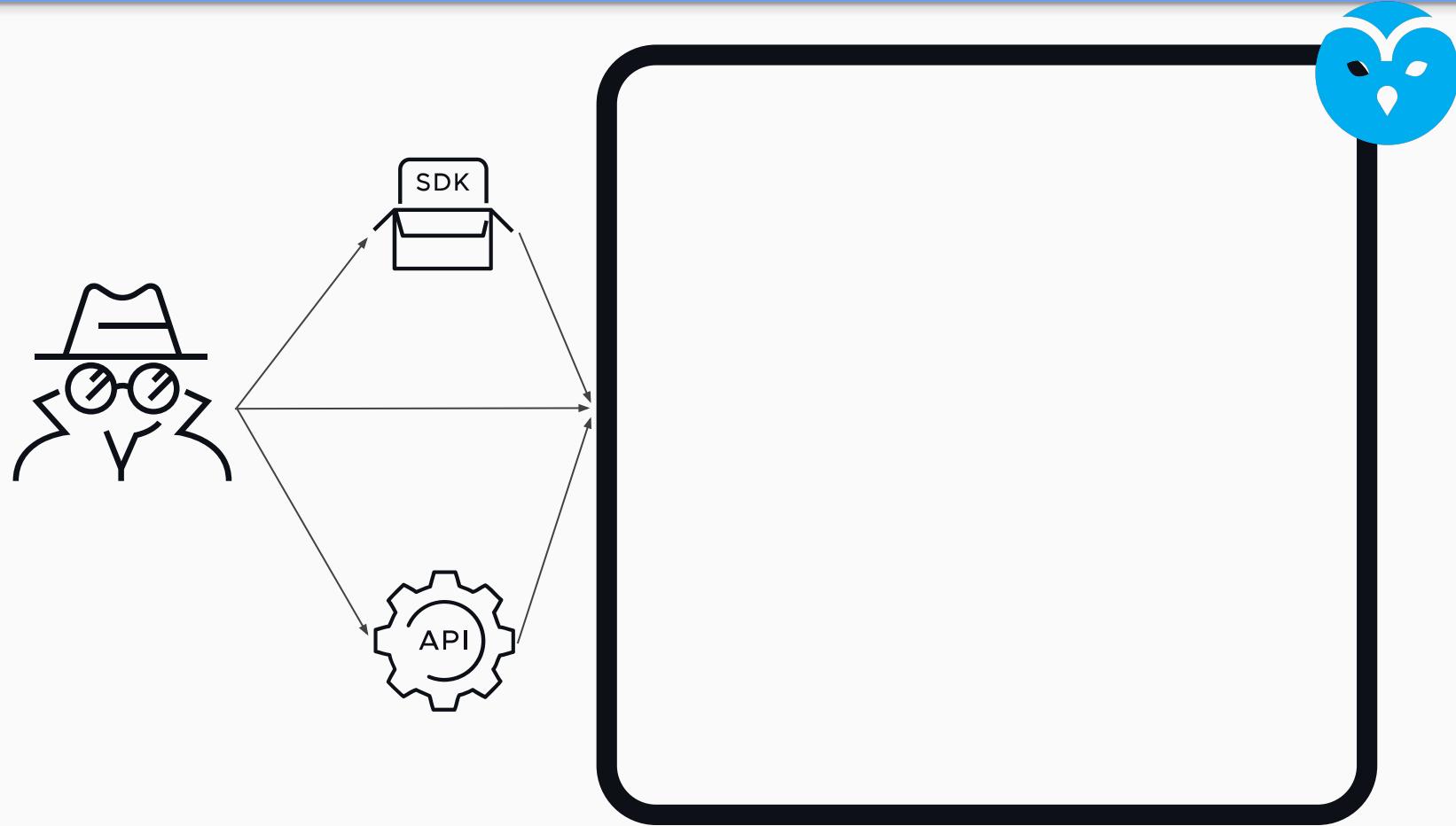
- Docker
- Python
- Django
- Django Rest Framework
- PostgreSQL
- ElasticSearch
- Nginx
- Uwsgi
- Rabbit-MQ/SQS
- ReactJS
- Celery



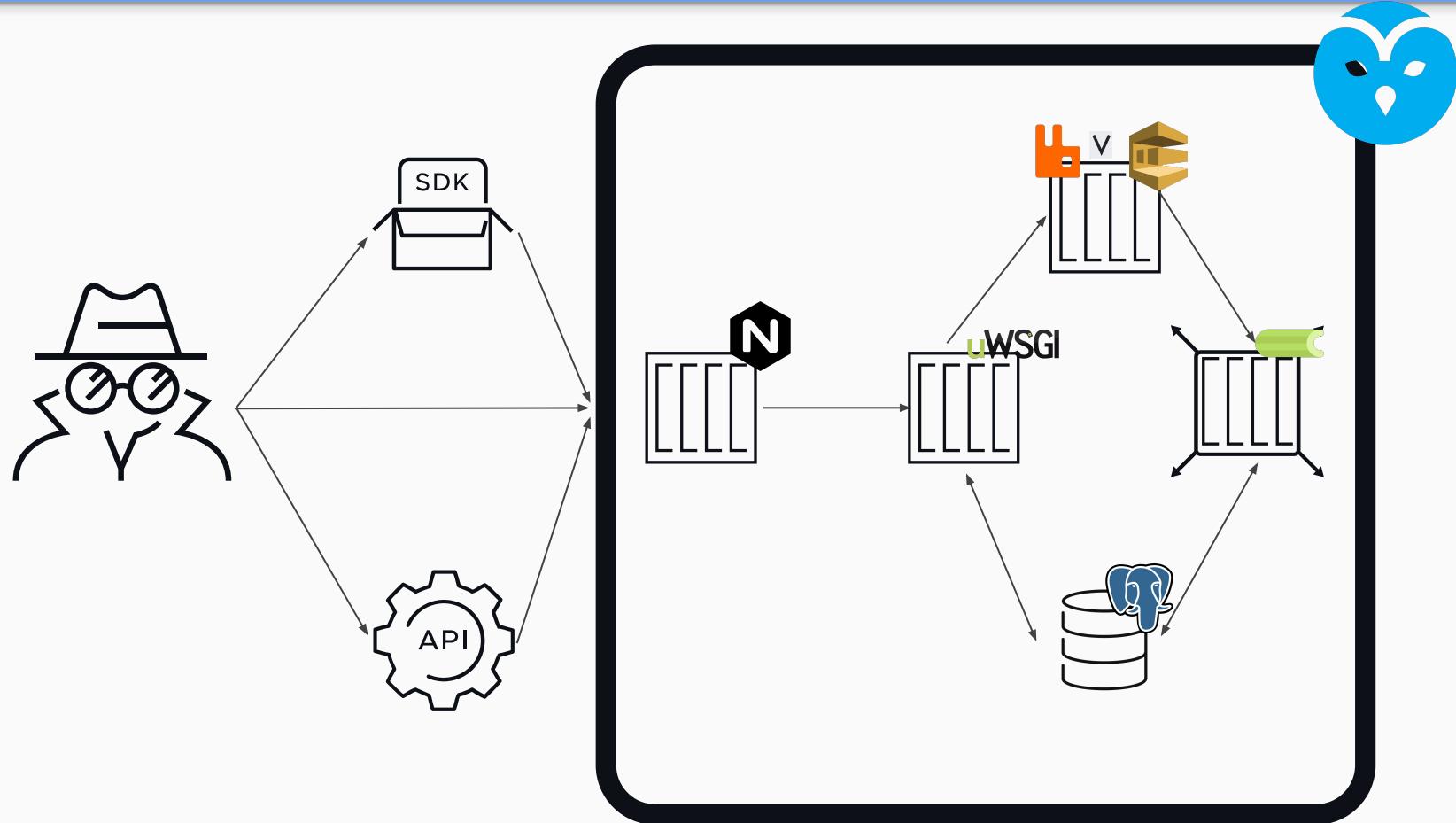


Analyst

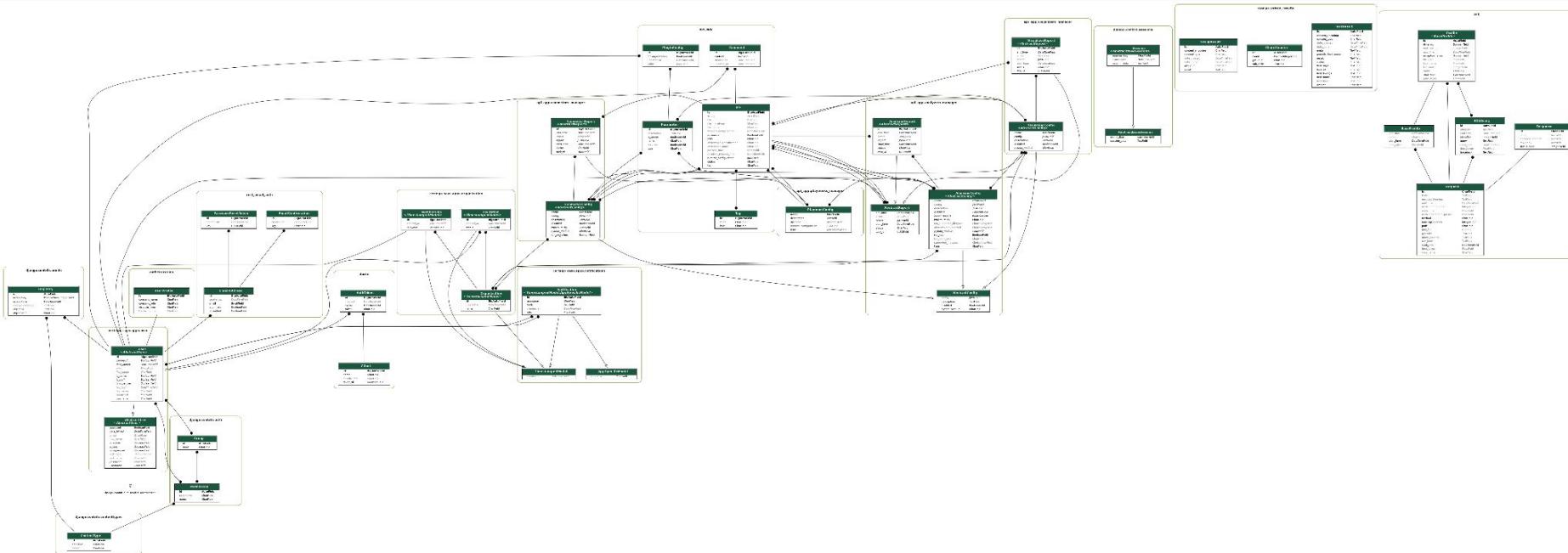




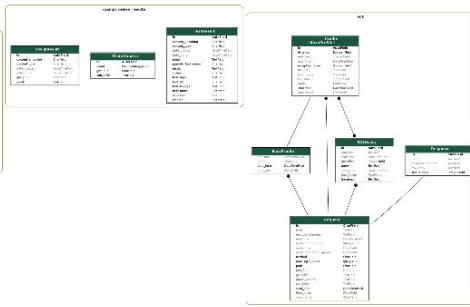
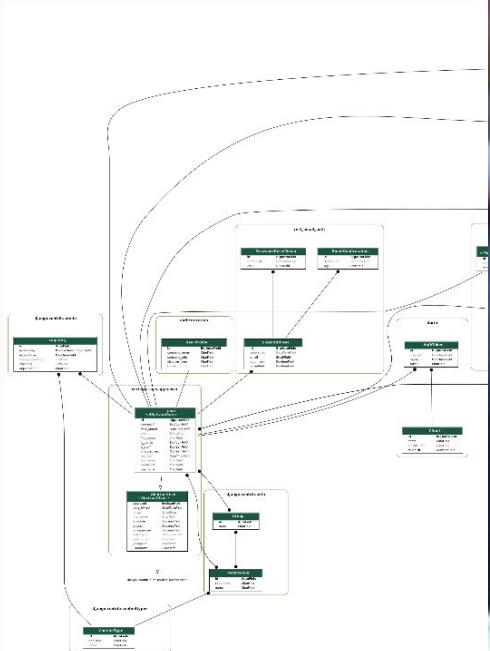
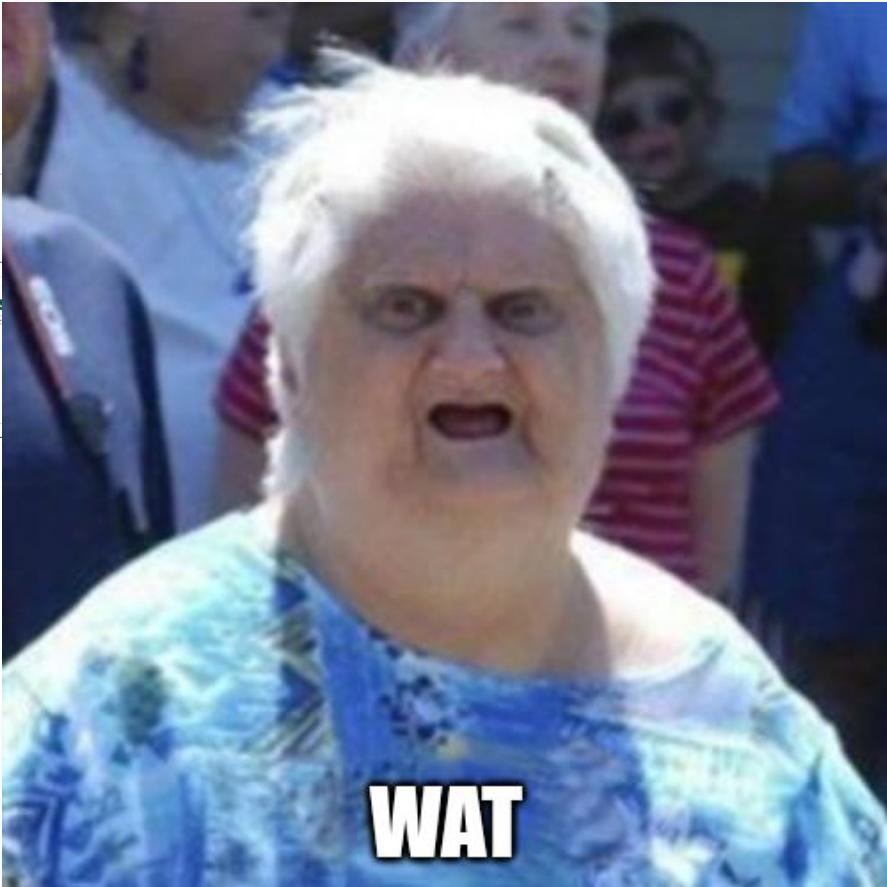
IntelOwl: Infrastructure Architecture



IntelOwl: Software Architecture



IntelOwl: Software Architecture



Easy and fast steps. Follow the official [documentation](#) (which we strive to keep up to date):

```
git clone https://github.com/intelowlproject/IntelOwl
cd IntelOwl/

# construct environment files from templates
cd docker/
cp env_file_app_template env_file_app
cp env_file_postgres_template env_file_postgres
cp env_file_integrations_template env_file_integrations

# (optional) verify installed dependencies
cd ..
./initialize.sh

# start the app
python3 start.py prod up

# create a super user
docker exec -ti intelowl_uwsgi python3 manage.py createsuperuser

# now you can login with the created user http://localhost:80

# Have fun!
```

Intel owl Home Dashboard Jobs Plugins Scan Docs 4 TE

Intel owl

Intel Owl is an Open Source Intelligence, or OSINT solution to get threat intelligence data about a specific file, an IP or a domain from a single API at scale. It integrates a number of analyzers available online and a lot of cutting-edge malware analysis tools. It is for everyone who needs a single point to query for info about a specific file or observable.

IntelOwl News

IntelOwl: Release v4.0.0 1st July 2022
Certego Blog: v4.0.0 Announcement
[Read](#)

IntelOwl: Release v3.0.0 13th September 2021
Honeynet Blog: v3.0.0 Announcement
[Read](#)

Intel Owl – OSINT tool automates the intel-gathering process using a single API 18th August 2020
Daily Swig: Interview with Matteo Lodi and Eshaan Bansal
[Read](#)

Intel owl Home Dashboard Jobs Plugins Scan Docs TE 3

Month: 44 Total: 45 ⓘ

Scan Observables

observable (domain, IP, URL, HASH, etc...) file

Observable Value(s) *

s8.svchostok.pro trash

Add new value

Playbooks Analyzers/Connectors

Select Playbooks

FREE_TO_USE_ANALYZERS 1/2 X ▼

Advanced settings

Start Scan

IntelOwl: Job Result (Raw Data) 1/2

Intel Owl Home Dashboard Jobs Plugins Scan Docs 3 TE

Job #2 ⚠

Domain: s8.svchostok.pro domain

Status: REPORTED WITH FAILS	TLP: CLEAR	User: test	MD5: f9bc35a57b22f82c94dbcc420f71b903	Process Time (mm:ss): 01:00	Start Time: 07:10:14 PM May 16th, 2023	End Time: 07:11:15 PM May 16th, 2023
Tags	Error(s)	Playbook: FREE_TO_USE_ANALYZERS				

Analyzers Report 20 / 20 Connectors Report 0 / 0 Visualizers Report 1 / all Visualizer Raw

	Actions	Status	Name	Process Time (s)	Running Time
✓		SUCCESS	URLhaus	0.19	7:10:14 PM - 7:10:15 PM (GMT+2)
✓		SUCCESS	Tranco	1.3	7:10:15 PM - 7:10:16 PM (GMT+2)
✓		SUCCESS	ThreatFox	0.24	7:10:14 PM - 7:10:15 PM (GMT+2)
✓		SUCCESS	Quad9_Malicious_Detector	0.11	7:10:15 PM - 7:10:15 PM (GMT+2)
✓		SUCCESS	Quad9_DNS	0.24	7:10:14 PM - 7:10:15 PM (GMT+2)
✓		SUCCESS	Mnemonic_PassiveDNS	0.67	7:10:15 PM - 7:10:15 PM (GMT+2)
✓		SUCCESS	MalwareBazaar_Google_Observable	3.6	7:10:15 PM - 7:10:18 PM (GMT+2)
✓		SUCCESS	Google	0.22	7:10:15 PM - 7:10:15 PM (GMT+2)

IntelOwl: Job Result (Raw Data) 2/2

Analyzers Report 20/20 Connectors Report 0/0 Visualizers Report 1/all						Visualizer	Raw
	Actions	Status	Name	Process Time (s)	Running Time		
		All	Search keyword...				
▼		SUCCESS	URLhaus	0.19	7:10:14 PM - 7:10:15 PM (GMT+2)		
▼		SUCCESS	Tranco	1.3	7:10:15 PM - 7:10:16 PM (GMT+2)		
^		SUCCESS	ThreatFox	0.24	7:10:14 PM - 7:10:15 PM (GMT+2)		

```
{
  "report": {
    "data": [
      {
        "id": "1117431",
        "ioc": "https://s8.svchostok.pro/fwlink",
        "tags": [...],
        "malware": "win.cobalt_strike",
        "ioc_type": "url",
        "reporter": "drb_ra",
        "last_seen": null,
        "reference": null,
        "first_seen": "2023-05-16 16:08:45 UTC",
        "threat_type": "botnet_cc",
        "ioc_type_desc": "URL that is used for botnet Command&Control (C&C)",
        "malware_alias": "Agentemis,BEACON,CobaltStrike,cobeacon"
      }
    ]
  }
}
```

▼		SUCCESS	Quad9_Malic	1 2 »	0.11	7:10:15 PM - 7:10:15 PM (GMT+2)
▼		SUCCESS	Quad9_DNS		0.24	7:10:14 PM - 7:10:15 PM (GMT+2)

IntelOwl: Job Result (Visualizers)

Intel Owl Home Dashboard Jobs Plugins Scan Docs 3 TE

Job #2 ⚠

Comments (0) Delete Job Rescan Save As Playbook Raw JSON Share

Domain s8.svchostok.pro

Status	TLP	User	MDS	Process Time (mm:ss)	Start Time	End Time
REPORTED WITH FAILS	CLEAR	test	f9bc35a57b22f82c94dbcc420f71b903	01:00	07:10:14 PM May 16th, 2023	07:11:15 PM May 16th, 2023

Tags Error(s) Playbook FREE_TO_USE_ANALYZERS

DNS Visualizer Raw

Classic DNS (2)
172.67.155.34
104.21.34.60

CloudFlare DNS (2)
104.21.34.60
172.67.155.34

DNS0 EU (0)

Google DNS (2)
172.67.155.34
104.21.34.60

Quad9 DNS (2)
172.67.155.34
104.21.34.60

CloudFlare Malicious Detector DNS0 EU Malicious Detector Quad9 Malicious Detector

IntelOwl: Plugins (Analyzers)

Intel owl Home Dashboard Jobs Plugins Scan Docs 3 TE

Analyzers 149 total

Analyzers are the most important plugins in IntelOwl. They allow to perform data extraction on the observables and/or files that you would like to analyze.

Note: Hover over a configured icon to view configuration status and errors if any.

Info	Name	Active	Configured	Enabled for organization	Description	Type	Supported types	Maximum TLP	Health Check
ⓘ	APKID	✓	✓	ⓘ	APKID identifies many compilers, packers, obfuscators, and other weird stuff from an APK or DEX file.	file	<ul style="list-style-type: none">• android• application/java-archive• application/vnd.android.package-archive• application/x-dex• application/zip	RED	ⓘ
ⓘ	AbuseIPDB	✓	✗	ⓘ	check if an ip was reported on AbuseIPDB	observable	<ul style="list-style-type: none">• ip	AMBER	
ⓘ	Anomali_Threatstream	✓	✗	ⓘ	Analyzer to interact with Anomali ThreatStream APIs	observable	<ul style="list-style-type: none">• domain• generic• hash• ip• url	AMBER	
ⓘ	Auth0	✓	✗	ⓘ	scan an IP against the Auth0 API	observable	<ul style="list-style-type: none">• ip	AMBER	
ⓘ	BinaryEdge	✓	✗	ⓘ	Details about an Host. List of recent events for the specified host, including details of exposed ports and services and return list of subdomains known from the target domains	observable	<ul style="list-style-type: none">• domain• ip	AMBER	
ⓘ	BitcoinAbuse	✓	✗	ⓘ	1 2 3 4 5 ... » bitcoinabuse.com, a public	observable	<ul style="list-style-type: none">• hash	AMBER	

IntelOwl: Plugins (Connectors)

Intel Owl Home Dashboard Jobs Plugins Scan Docs 3 TE

Analyzers Connectors Visualizers Playbooks Your plugin config

Connectors 4 total

Connectors are designed to run after every successful analysis which makes them suitable for automated threat-sharing. They support integration with other SIEM/SOAR projects, specifically aimed at Threat Sharing Platforms.

Note: Hover over a configured icon to view configuration status and errors if any.

Info	Name	Active	Configured	Enabled for organization	Description	Maximum TLP	Health Check
	MISP				Automatically creates an event on your MISP instance, linking the successful analysis on IntelOwl	CLEAR	
	OpenCTI				Automatically creates an observable and a linked report on your OpenCTI instance, linking the successful analysis on IntelOwl	CLEAR	
	Slack				Send the analysis link to a slack channel	RED	
	YETI				find or create observable on YETI, linking the successful analysis on IntelOwl.	CLEAR	

IntelOwl: Plugins (Playbooks)

Intel Owl Home Dashboard Jobs Plugins Scan Docs 3 TE

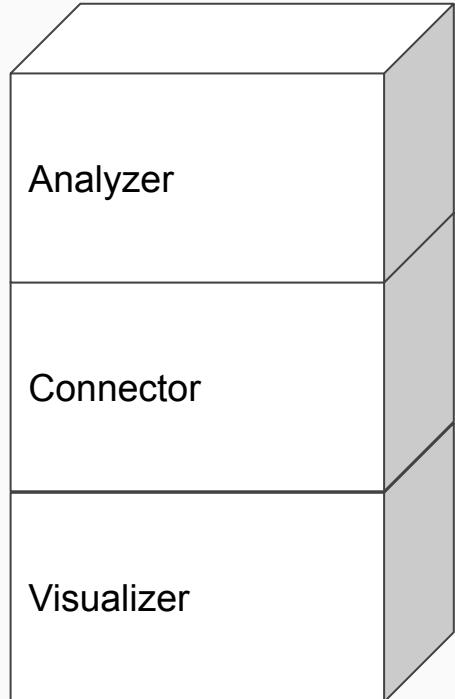
Analyzers Connectors Visualizers Playbooks Your plugin config

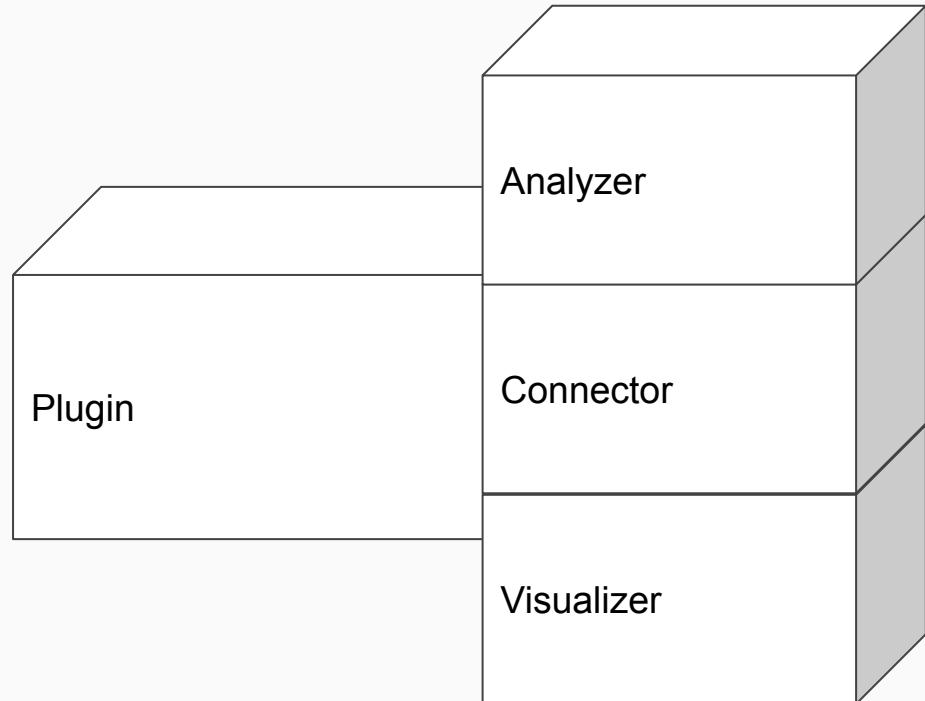
Playbooks 1 total

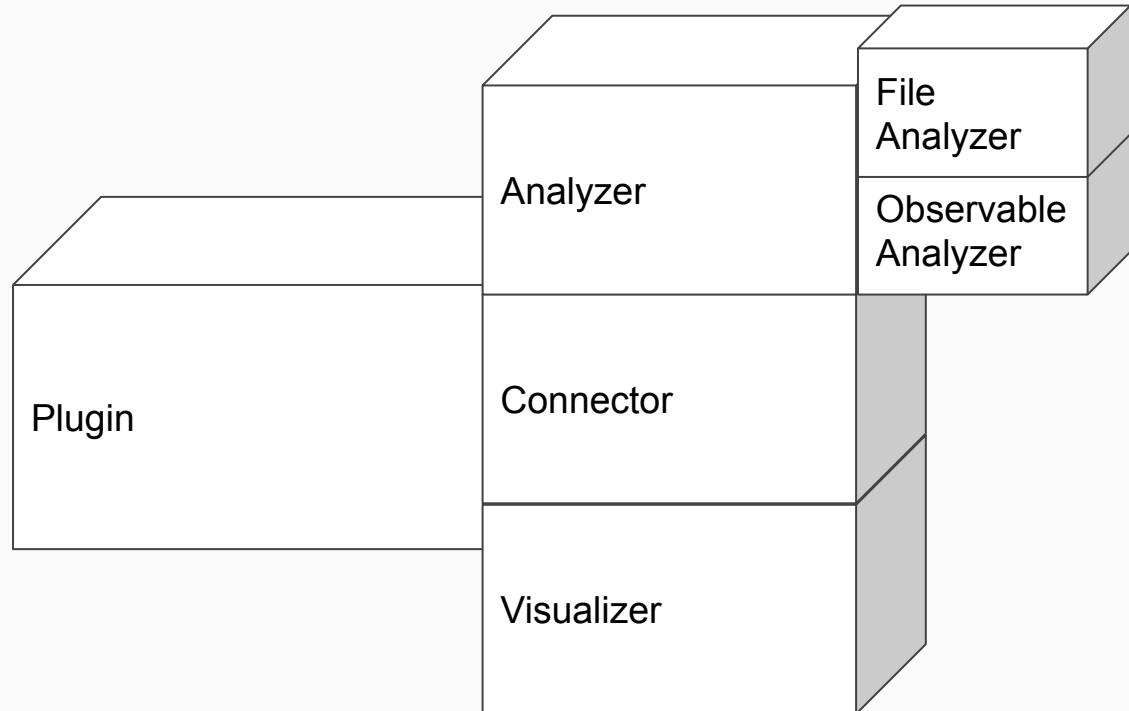
Playbooks are designed to be easy to share sequence of running Analyzers/Connectors on a particular kind of observable.

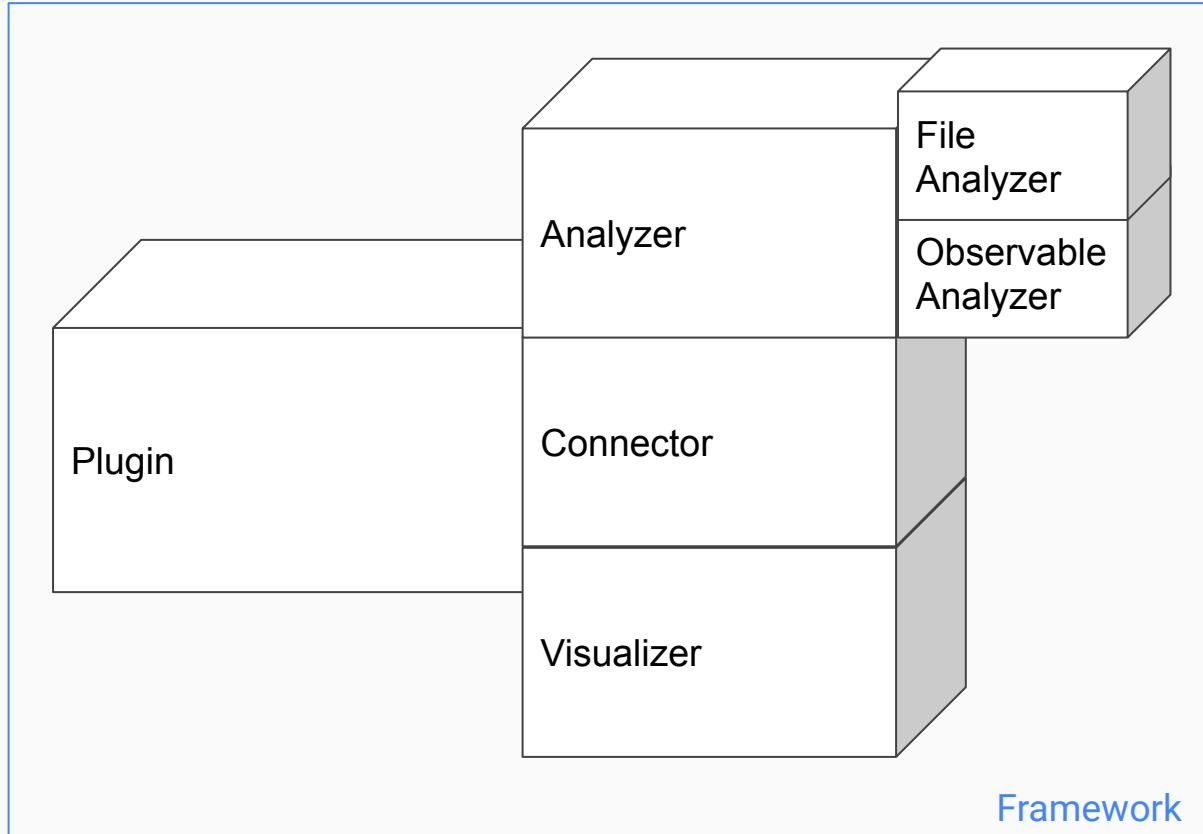
Note: Hover over a configured icon to view configuration status and errors if any.

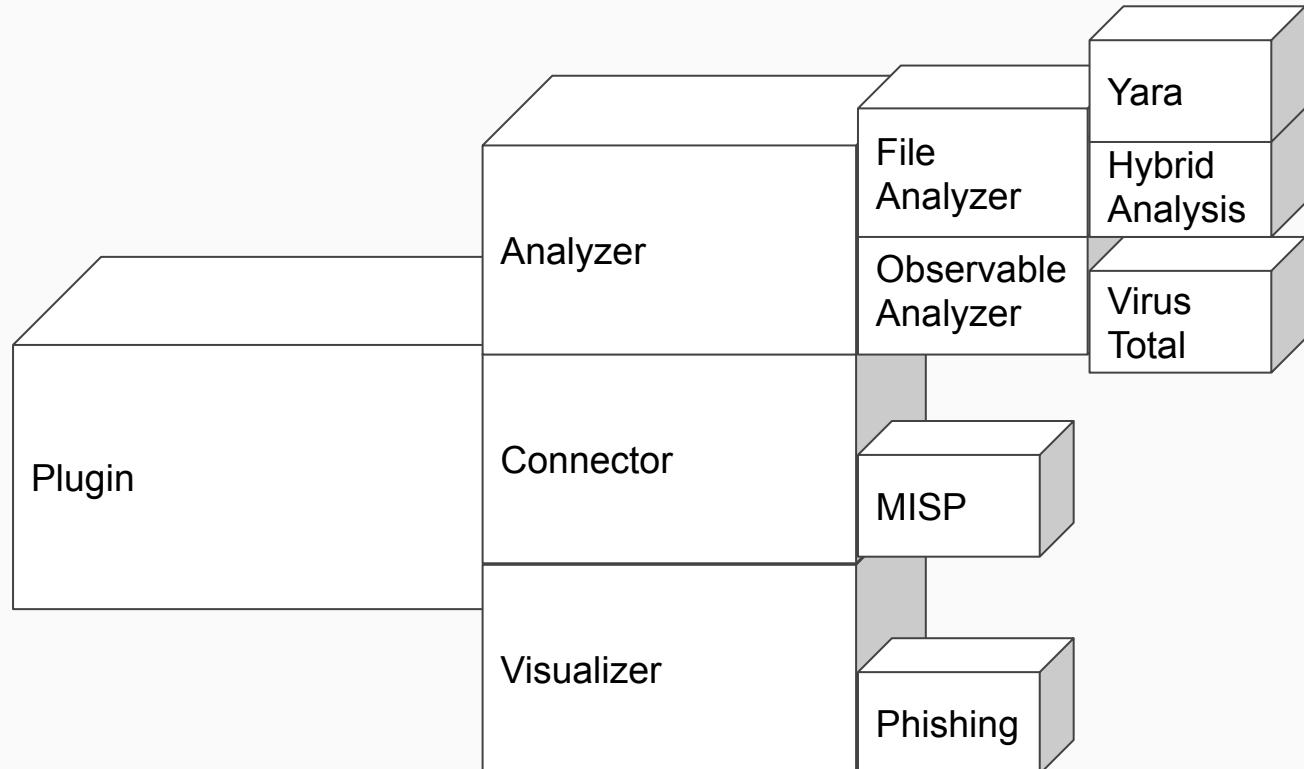
Info	Name	Active	Description	Type	Analyzers executed	Connectors executed
	Sample Static Analysis		Execute a static analysis	["file"]	<ul style="list-style-type: none">APKIDBoxJS_Scan_JavaScriptClamAVCymru_Hash_Registry_Get_FDoc_InfoHybridAnalysis_Get_FileMalwareBazaar_Get_FileOTX_Check_HashOneNote_InfoPDF_InfoQuark_EngineRtf_InfoYARAify_File_SearchYara	All

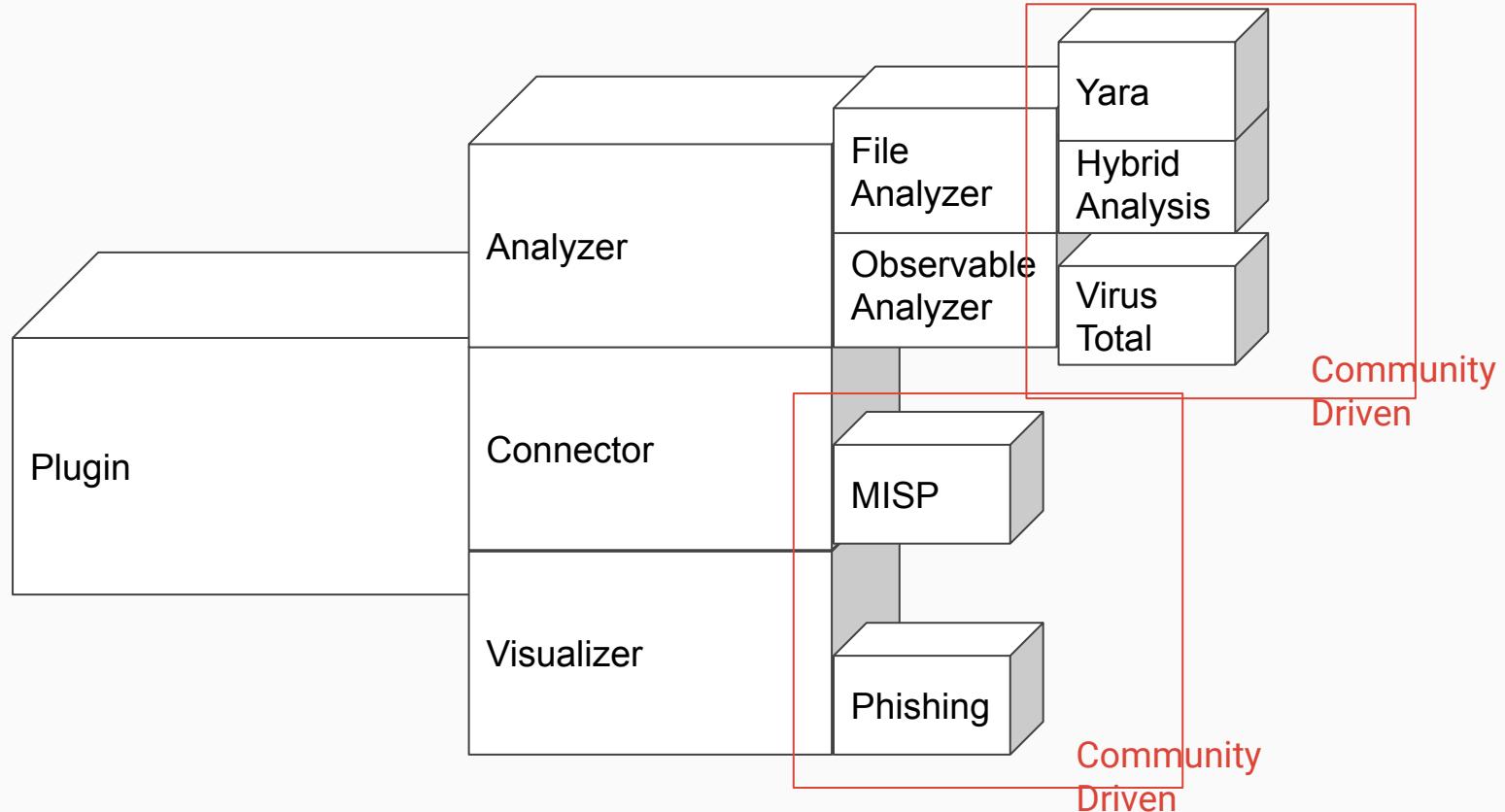












Plugin



Community
Driven

Driven

Intel owl Home Dashboard Jobs Plugins Scan Docs TE 3

Month: 44 Total: 45 ⓘ

Scan Observables

observable (domain, IP, URL, HASH, etc...) file

Observable Value(s) *

s8.svchostok.pro trash

Add new value

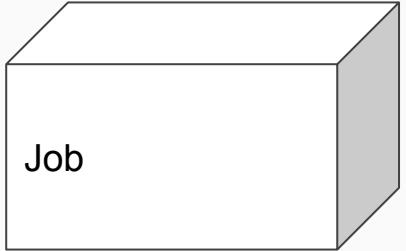
Playbooks Analyzers/Connectors

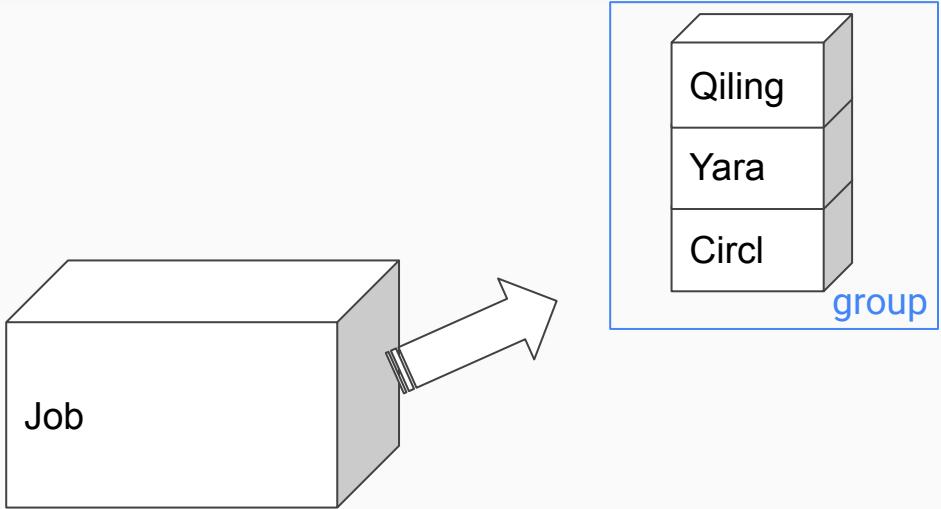
Select Playbooks

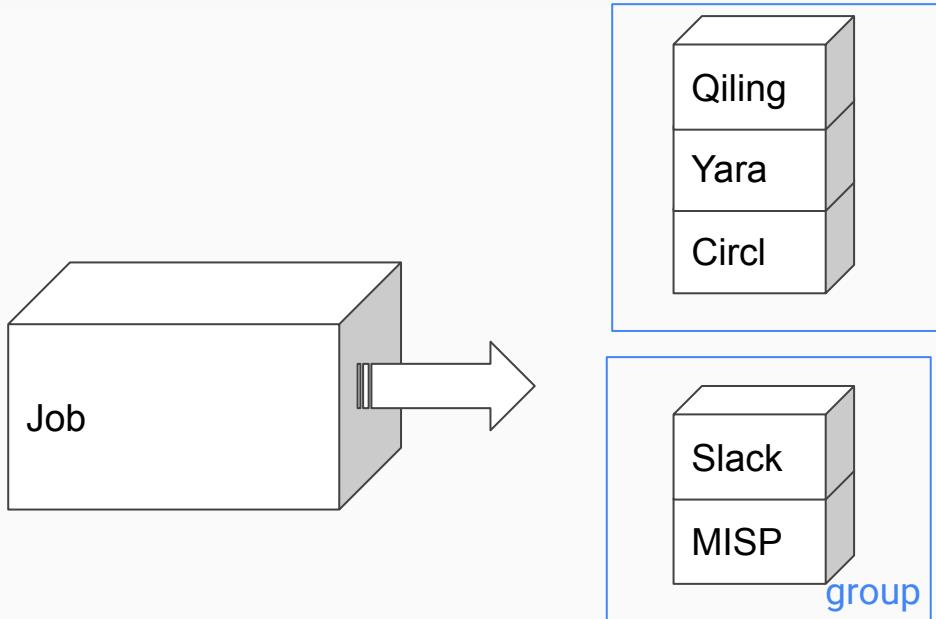
FREE_TO_USE_ANALYZERS 1/2 X ▼

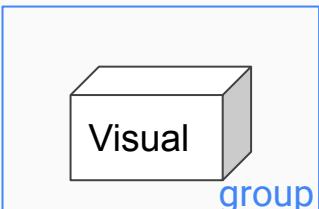
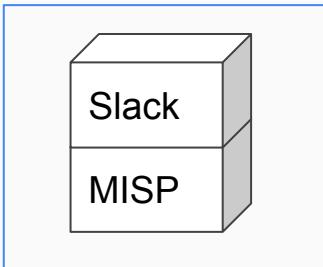
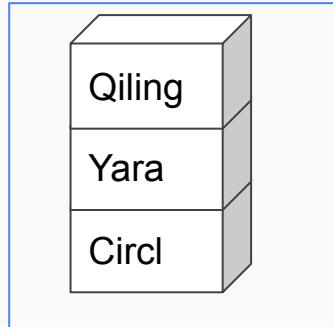
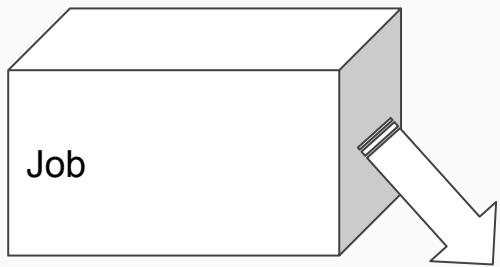
Advanced settings ⓘ

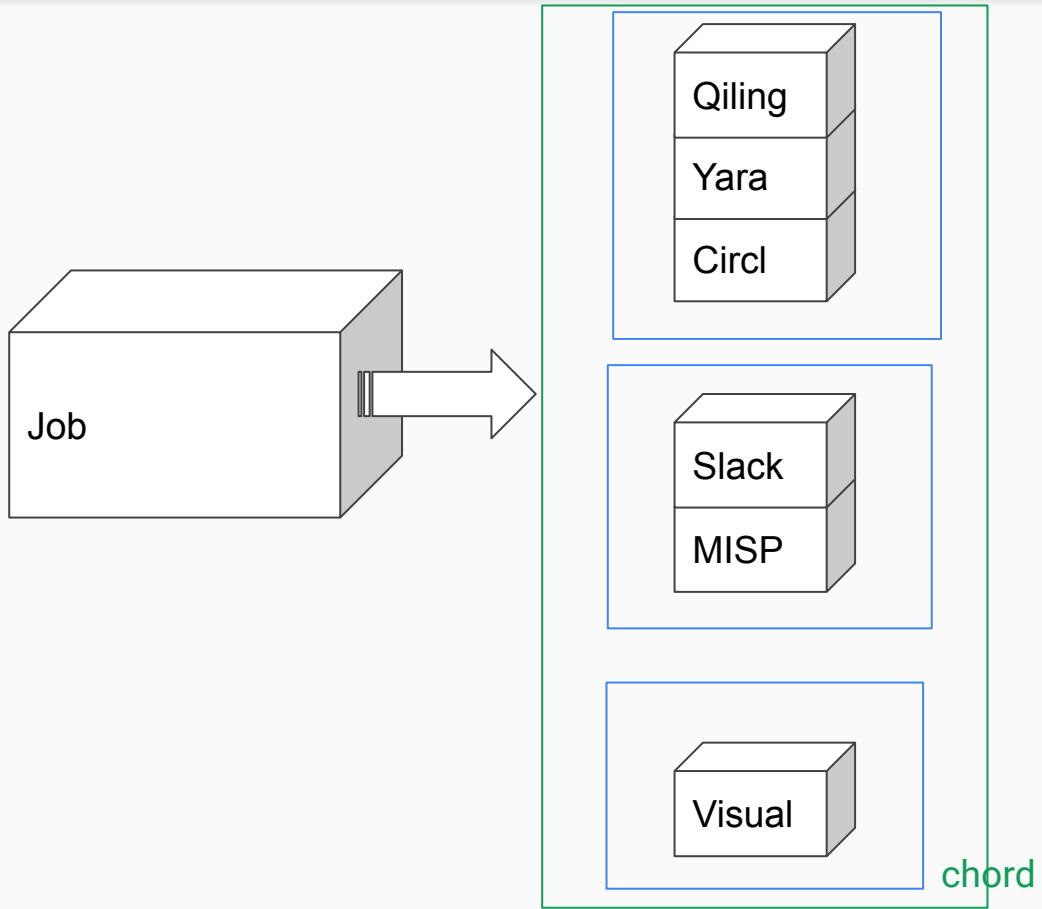
Start Scan

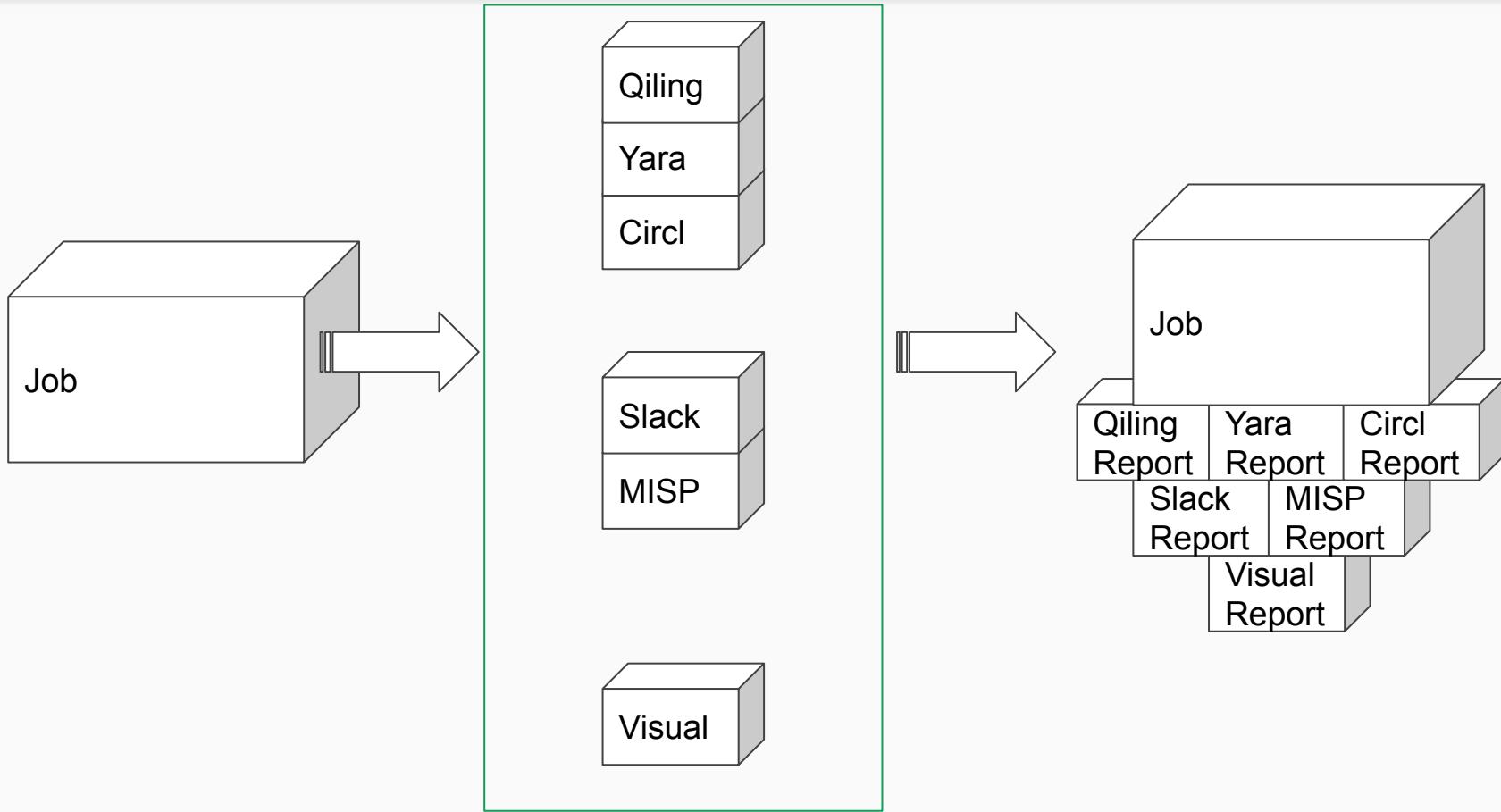












IntelOwl: Job Result (Raw Data)

Intel Owl Home Dashboard Jobs Plugins Scan Docs 3 TE

Job #2 ⚠

Domain: s8.svchostok.pro

Status: REPORTED WITH FAILS	TLP: CLEAR	User: test	MD5: f9bc35a57b22f82c94dbcc420f71b903	Process Time (mm:ss): 01:00	Start Time: 07:10:14 PM May 16th, 2023	End Time: 07:11:15 PM May 16th, 2023
Tags:	Error(s):	Playbook: FREE_TO_USE_ANALYZERS				

Analyzers Report 20 / 20 Connectors Report 0 / 0 Visualizers Report 1 / all

Visualizer Raw

	Actions	Status	Name	Process Time (s)	Running Time
✓		SUCCESS	URLhaus	0.19	7:10:14 PM - 7:10:15 PM (GMT+2)
✓		SUCCESS	Tranco	1.3	7:10:15 PM - 7:10:16 PM (GMT+2)
✓		SUCCESS	ThreatFox	0.24	7:10:14 PM - 7:10:15 PM (GMT+2)
✓		SUCCESS	Quad9_Malicious_Detector	0.11	7:10:15 PM - 7:10:15 PM (GMT+2)
✓		SUCCESS	Quad9_DNS	0.24	7:10:14 PM - 7:10:15 PM (GMT+2)
✓		SUCCESS	Mnemonic_PassiveDNS	0.67	7:10:15 PM - 7:10:15 PM (GMT+2)
✓		SUCCESS	MalwareBazaar_Google_Observable	3.6	7:10:15 PM - 7:10:18 PM (GMT+2)
✓		SUCCESS	Google	0.22	7:10:15 PM - 7:10:15 PM (GMT+2)



You get a link to an URL inside a suspicious email. Could it be phishing?

IntelOwl is integrated with tons of external services which can be queried to understand whether an URL is malicious or not and which kind of threat it poses: Reputation Services, DNS Resolvers, WHOIS services, Passive DNS services, URL Sandboxes, Threat Intel Platforms, Information Sharing Platforms, etc

Those are all pre-built in the default installation.

The screenshot shows the 'Scan Observables' section of the IntelOwl web interface. At the top, there are two radio button options: 'observable (domain, IP, URL, HASH, etc...)' (selected) and 'file'. Below this is a field labeled 'Observable Value(s) *' containing the URL 'http://mspmotoworld.com'. To the right of the URL input is a blue trash can icon. Underneath the URL input is a blue button with a plus sign and the text 'Add new value'. Further down, there are two more radio button options: 'Playbooks' (selected) and 'Analyzers/Connectors'. At the bottom left, there is a 'Select Playbooks' dropdown menu with 'Popular URL Reputation Services' listed. At the bottom right, there is a navigation bar with '1/2', a close button 'x', and a dropdown arrow '▼'.

IntelOwl example use case: Phishing verification (2 / 3)

Intel owl Home Dashboard Jobs Plugins Scan Docs 5 TE

Job #175

http://mspmotoworld.com

Status	TLP	User	MD5	Process Time (mm:ss)	Start Time	End Time
REPORTED WITHOUT FAILS	CLEAR	test	a4f92c7273a3e828e9f68d33e249c35c	00:52	11:38:48 AM May 18th, 2023	11:39:41 AM May 18th, 2023

Tags Error(s) Playbook Popular URL Reputation Services

Reputation Visualizer Raw

VirusTotal ↗ Engine Hits: 26

Phishtank ↗ found

PhishingArmy ↗ found

URLhaus ↗

InQuest ↗ found

CloudFlare Malicious Detector

GoogleSafebrowsing

Quad9 Malicious Detector

OTX AlienVault (0)

DNS0 EU Malicious Detector

IntelOwl example use case: Phishing verification (3 / 3)

Analyzers Report 11/11 Connectors Report 0/0 Visualizers Report 1/all Visualizer Raw

	Actions	Status	Name	Process Time (s)	Running Time
▼		SUCCESS	VirusTotal_v3_Get_Observable	0.81	11:38:49 AM - 11:38:50 AM (GMT+2)
▼		SUCCESS	URLhaus	0.32	11:38:49 AM - 11:38:49 AM (GMT+2)
▼		SUCCESS	ThreatFox	0.36	11:38:49 AM - 11:38:49 AM (GMT+2)
▼		SUCCESS	Quad9_Malicious_Detector	0.58	11:38:49 AM - 11:38:50 AM (GMT+2)
▲		SUCCESS	Phishtank	0.53	11:38:49 AM - 11:38:49 AM (GMT+2)

▼ {
 "report": {
 "meta": {...}
 },
 "results": {
 "url": "http://mspmotoworld.com"
 "valid": true
 "phish_id": "8148103"
 "verified": true
 "in_database": true
 "verified_at": "2023-05-17T04:42:20+00:00"
 "phish_detail_page": "http://www.phishtank.com/phish_detail.php?phish_id=8148103"
 }
}
"errors": []
"runtime_configuration": {}

1 2 »

You get a list of IP addresses that have been doing a lot of connections against your infrastructure. Are they legit scanners (crawlers like GoogleBot) or are they known to be abused?

IntelOwl is integrated with tons of external services which can be queried to understand whether an IP address is malicious or not and which kind of threat it poses: Reputation Services, DNS Resolvers, Passive DNS services, Threat Intel Platforms, Information Sharing Platforms, etc

Scan Observables

observable (domain, IP, URL, HASH, etc...) file

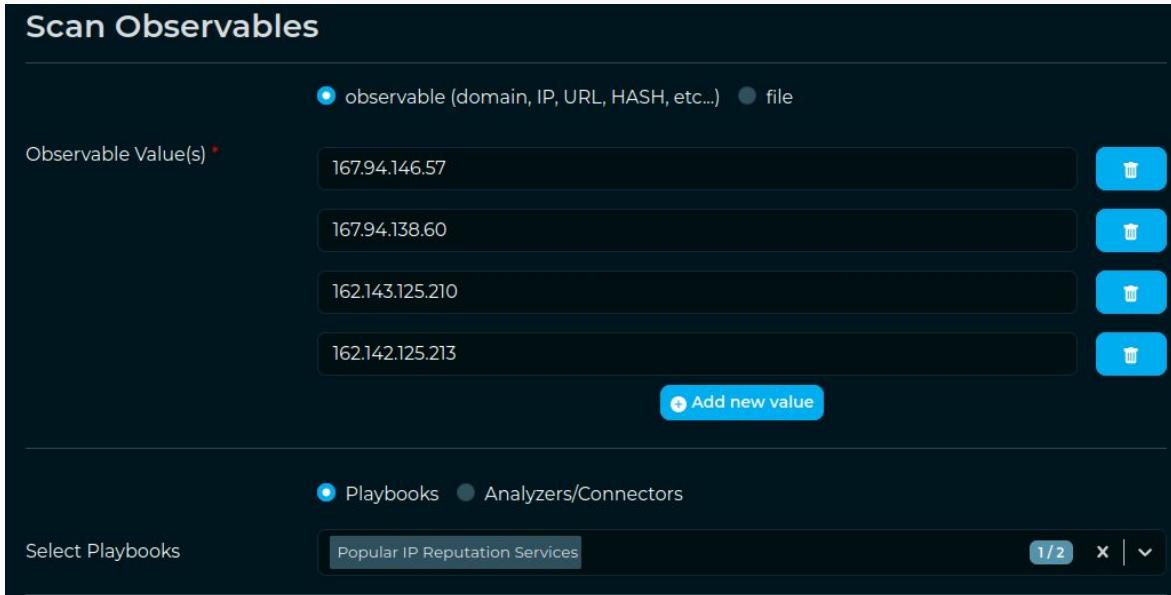
Observable Value(s) *

- 167.94.146.57 Delete
- 167.94.138.60 Delete
- 162.143.125.210 Delete
- 162.142.125.213 Delete

[Add new value](#)

Playbooks Analyzers/Connectors

Select Playbooks Popular IP Reputation Services 1/2 x | v



IntelOwl example use case: Filtering of legit connections (2 / 3)

167.94.146.57 ip

Status	TLP	User	MD5	Process Time (mm:ss)	Start Time	End Time
REPORTED WITHOUT FAILS	CLEAR	test	91e8ef8d3e22316301d5e57102e0660b	00:30	06:22:48 PM May 18th, 2023	06:23:19 PM May 18th, 2023

Tags Error(s) Playbook Popular IP Reputation Services

Reputation Visualizer Raw

VirusTotal Engine Hits: 0

Greynoise Censys

AbuseIPDB Categories (9) Port Scan Web App Attack Bad Web Bot Brute Force Exploited Host

Crowdsec Behaviors (4) POP3/IMAP Bruteforce SIP Bruteforce HTTP Scan HTTP Exploit

OTX AlienVault (20) Ka's Honeypot visitors Webscanners with Bad Requests - HTTP Status 400 - 1/20/2018 thru current day IP Addresses Logged by the Rosethorn PotNet WEB Attack Known Pattern LCIA:HoneyNet:2023

AbuseIPDB Meta Censys Inc. (Search Engine Spider)

FireHol (0)

Tor Exit Node

Talos Reputation

IntelOwl example use case: Filtering of legit connections (3 / 3)

```
SUCCESS
AbuseIPDB
{
  "report": {
    "data": {
      "isp": "Censys Inc.",
      "domain": "censys.io",
      "reports": [
        [ 0 - 100 ],
        [ 100 - 200 ]
      ],
      "isPublic": true,
      "hostnames": [...],
      "ipAddress": "162.142.125.213",
      "ipVersion": 4,
      "usageType": "Search Engine Spider",
      "countryCode": "US",
      "countryName": "United States of America",
      "totalReports": 3440,
      "isWhitelisted": true
    }
  }
}
```

« 1 2 3 4 5 »

You get a possible malicious file and you need to understand more about it.

IntelOwl embeds a high number of open source file analysis tools: Yara, ClamAV, Exiftools, Pdfld, Oletools, PeFile, Mandiant's Tools (Floss, Speakeasy, Stringsifter, CAPA), Quark Engine, Qiling, etc.

To leverage them all, you have to execute IntelOwl with an optional Docker container:

```
# start the app
python3 start.py prod up --malware_analysis_tools
```

Moreover IntelOwl is able to send either the sample or the hash only to external services for further analysis: VirusTotal, Intezer, etc

The screenshot shows the 'Scan Files' section of the IntelOwl web interface. At the top, there are two radio button options: 'observable (domain, IP, URL, HASH, etc...)' and 'file'. The 'file' option is selected. Below this is a 'File(s) *' input field containing 'Gandcrab.bin', with a 'Browse...' button to its left. Underneath the file input, there are two more radio buttons: 'Playbooks' (selected) and 'Analyzers/Connectors'. At the bottom left is a 'Select Playbooks' button, and at the bottom center is a 'Sample Static Analysis' button. In the bottom right corner, there is a navigation bar with '1/2', an 'X' button, and a dropdown arrow.

IntelOwl example use case: Suspicious File Analysis (2 / 4)

 **GandCrab.bin** file: application/x-dosexec

Status	TLP	User	MD5	Process Time (mm:ss)	Start Time	End Time
REPORTED WITH FAILS	CLEAR	b2	07fadb006486953439ce0092651fd7a6	00:00	04:49:28 PM May 17th, 2023	04:49:29 PM May 17th, 2023
Tags		Error(s)		Playbook		
				Sample Static Analysis		

Visualizer Raw

No visualizers available.

IntelOwl example use case: Suspicious File Analysis (2 / 4)

The screenshot shows the IntelOwl analysis interface for a file named "GandCrab.bin". The file type is listed as "file: application/x-dosexec". The analysis status is "REPORTED WITH FAILS". The TLP level is set to "CLEAR". The user who uploaded the file is "b2". The MD5 hash is "07fad...". The access time is "00:00". The start time is "04:49:28 PM May 17th, 2023". The end time is "04:49:29 PM May 17th, 2023". There are no tags or errors present. A "Playbook" button is available, along with a "Sample Static Analysis" link. At the bottom right, there are "Visualizer" and "Raw" options. A large, semi-transparent watermark reading "Help us pls" is overlaid on the interface.

GandCrab.bin file: application/x-dosexec

Status: REPORTED WITH FAILS

TLP: CLEAR

User: b2

MD5: 07fadb006486953439ca6...51fd7a6

Access Time (approx): 00:00

Start Time: 04:49:28 PM May 17th, 2023

End Time: 04:49:29 PM May 17th, 2023

Tags:

Error(s):

No visualizers available.

Playbook

Sample Static Analysis

Visualizer Raw

Help us pls

IntelOwl example use case: Suspicious File Analysis (3 / 4)

Gandcrab.bin file: application/x-dosexec

Status	TLP	User	MD5	Process Time (mm:ss)	Start Time	End Time
REPORTED WITH FAILS	CLEAR	test	07fadbd006486953439ce0092651fd7a6	00:52	12:56:00 PM May 18th, 2023	12:56:52 PM May 18th, 2023

Tags Error(s) Playbook Sample Static Analysis

Analyzers Report 8/8 Connectors Report 0/0 Visualizers Report 0/all Visualizer Raw

	Actions	Status	Name	Process Time (s)	Running Time
▼		All	Yara	0.72	12:56:00 PM - 12:56:00 PM (GMT+2)
▼		SUCCESS	Strings_Info	10.13	12:56:00 PM - 12:56:10 PM (GMT+2)
▼		SUCCESS	Signature_Info	0.09	12:56:00 PM - 12:56:00 PM (GMT+2)
▼		SUCCESS	PE_Info	0.26	12:56:00 PM - 12:56:00 PM (GMT+2)
▼		SUCCESS	Floss	20.2	12:56:00 PM - 12:56:20 PM (GMT+2)
▼		SUCCESS	ClamAV	3.06	12:56:00 PM - 12:56:03 PM (GMT+2)
▼		SUCCESS	Capa_Info	20.25	12:56:00 PM - 12:56:20 PM (GMT+2)

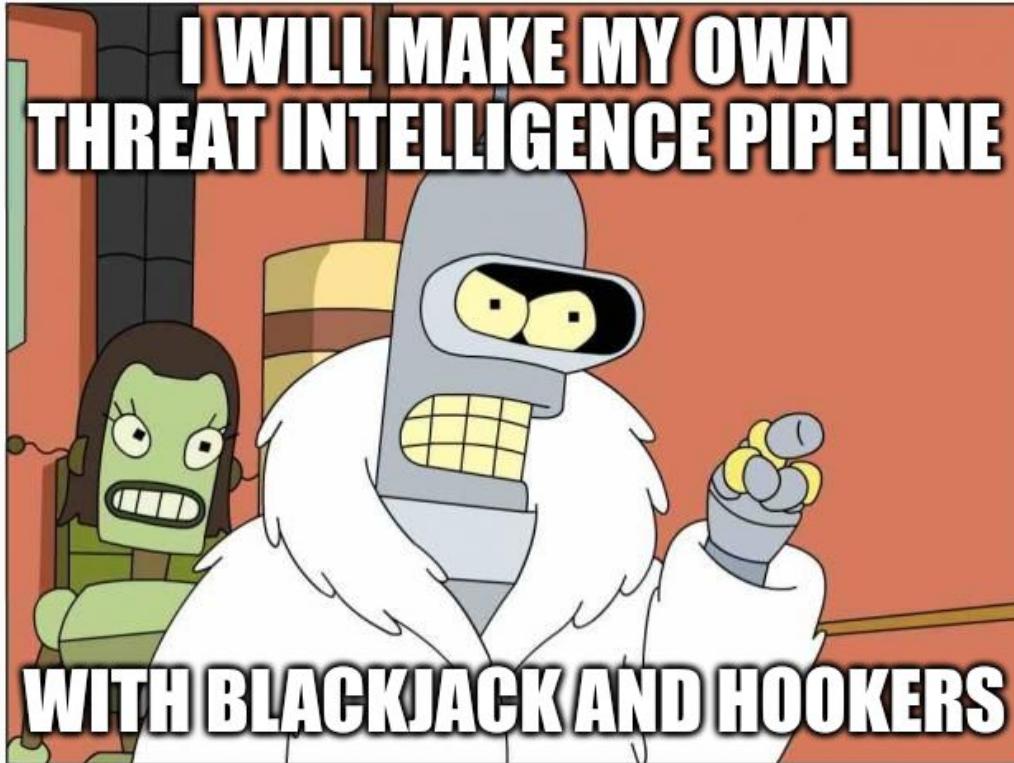
IntelOwl example use case: Suspicious File Analysis (4 / 4)

```
  {
    "report": {
      "detections": [
        0 : "Win.Exploit.CVE_2018_8440-6681865-1",
        1 : "Win.Ransomware.Gandcrab-6667060-0", [Redacted]
        2 : "Win.Malware.Razy-6829823-0",
        3 : "Win.Ransomware.Gandcrab-9764464-0"
      ]
    }
  }
```

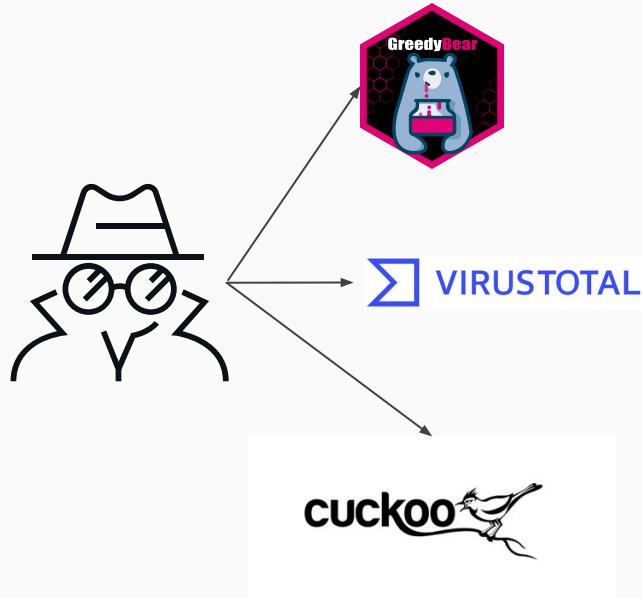
IntelOwl example use case: Suspicious File Analysis (4 / 4)

	SUCCESS	ClamAV	3.04	5:48:46 PM - 5:48:49 PM (GMT+2)
{ "report" : { "detections" : [0 : "Win.Exploit.CVE_2018_8440-6681865-1" 1 : "Win.Ransomware.Gandcrab-6667060-0" 2 : "Win.Malware.Razy-6829823-0" 3 : "Win.Ransomware.Gandcrab-9764464-0"] } }				

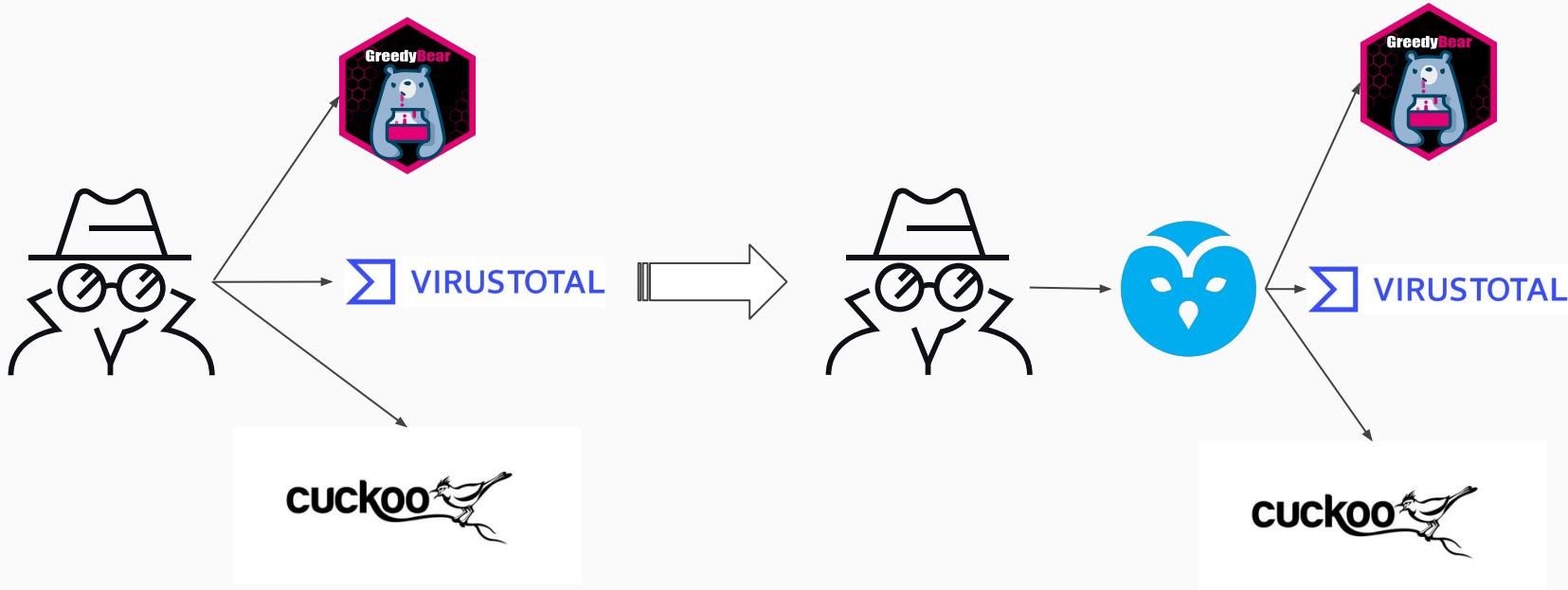
	SUCCESS	Yara	0.51	4:49:28 PM - 4:49:29 PM (GMT+2)
{ "jpcertcc_jpcert-yara" : [], "sbousseaden_yarahunts" : [], "neo23x0_signature-base" : [0 : { "url" : "https://github.com/Neo23x0/signature-base.git", "meta" : {...}, "path" : "/opt/deploy/files_required/yara/neo23x0_signature-base/yara/crime_ransom_generic.yar", "tags" : [], "match" : "SUSP_RANSOMWARE_Indicator_Jul20" }] }				



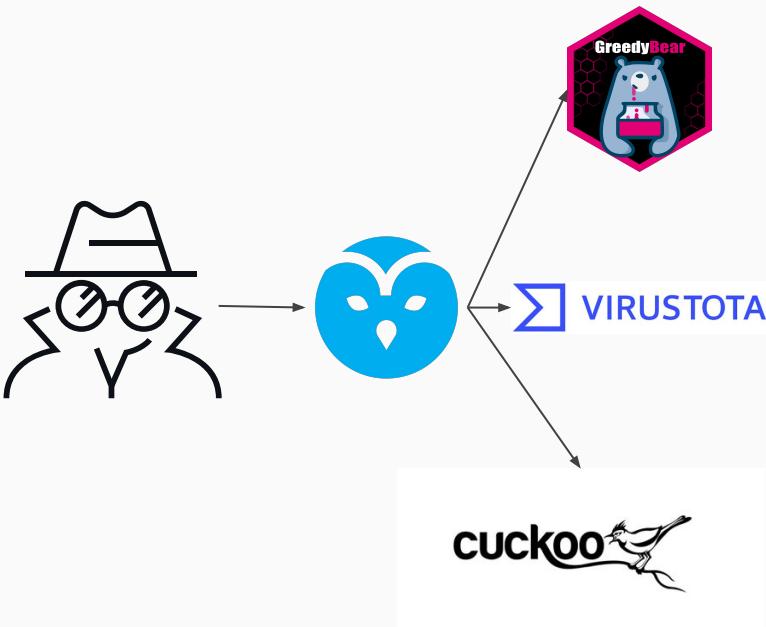
A Threat Intelligence pipeline with IntelOwl (1 / 3)



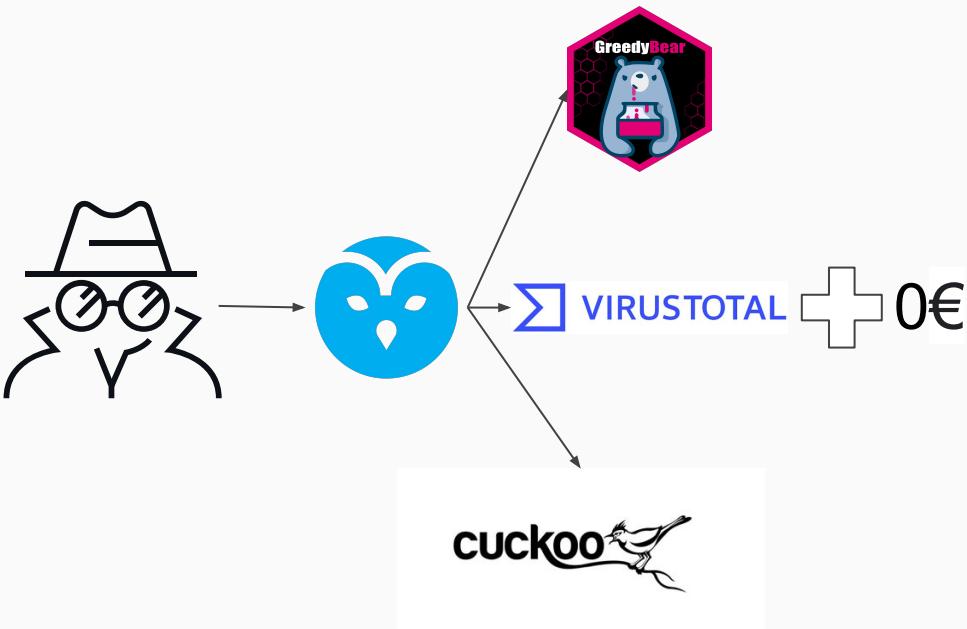
A Threat Intelligence pipeline with IntelOwl (1 / 3)



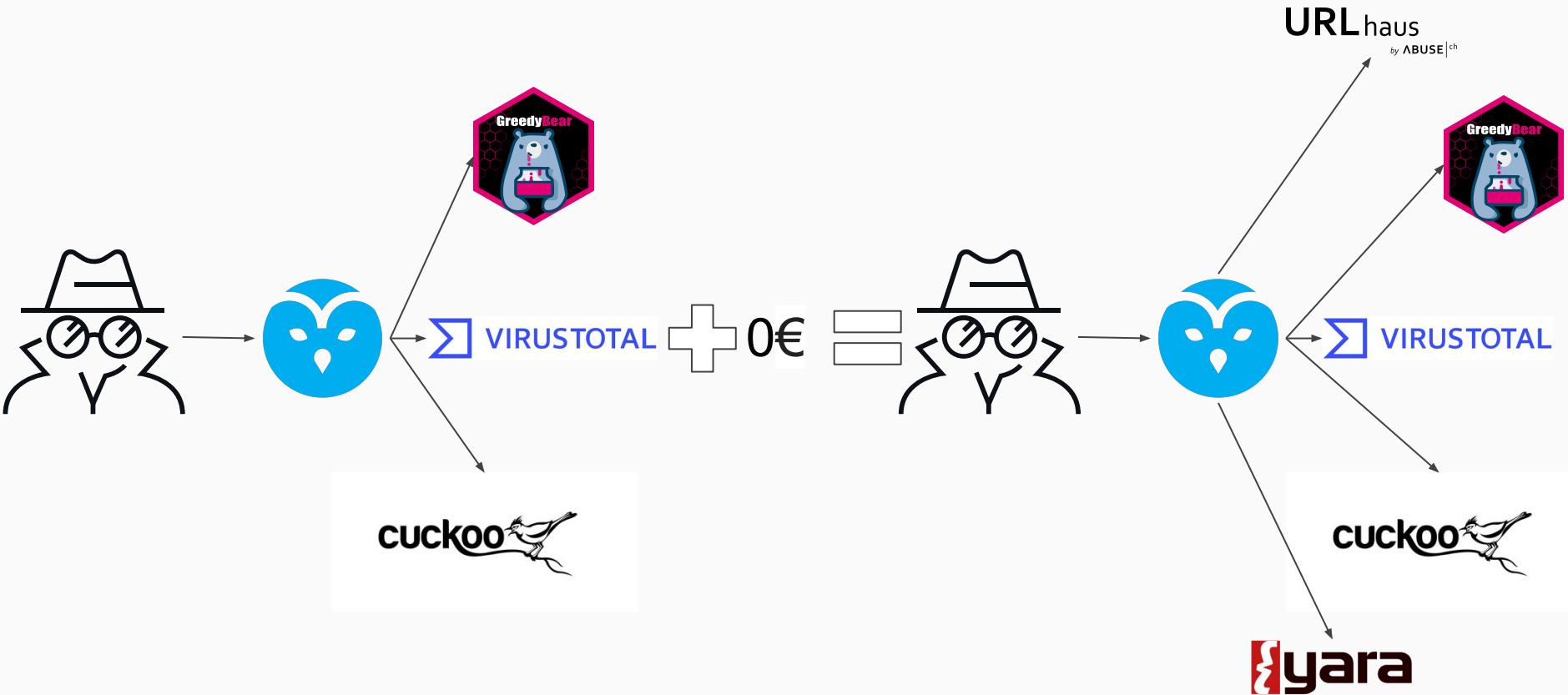
A Threat Intelligence pipeline with IntelOwl (2 / 3)



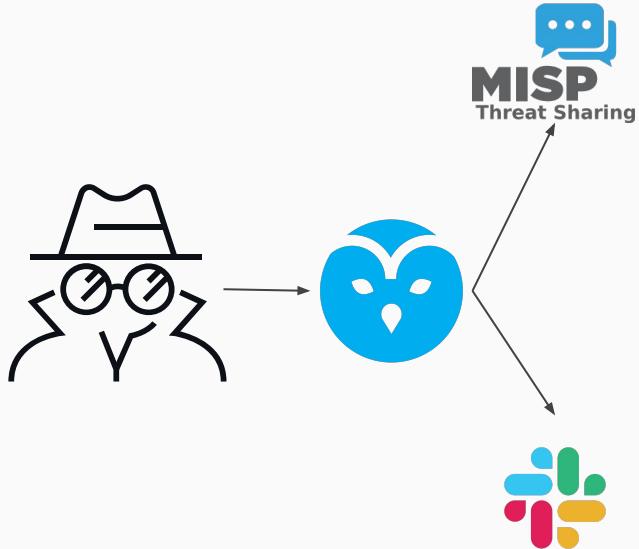
A Threat Intelligence pipeline with IntelOwl (2 / 3)



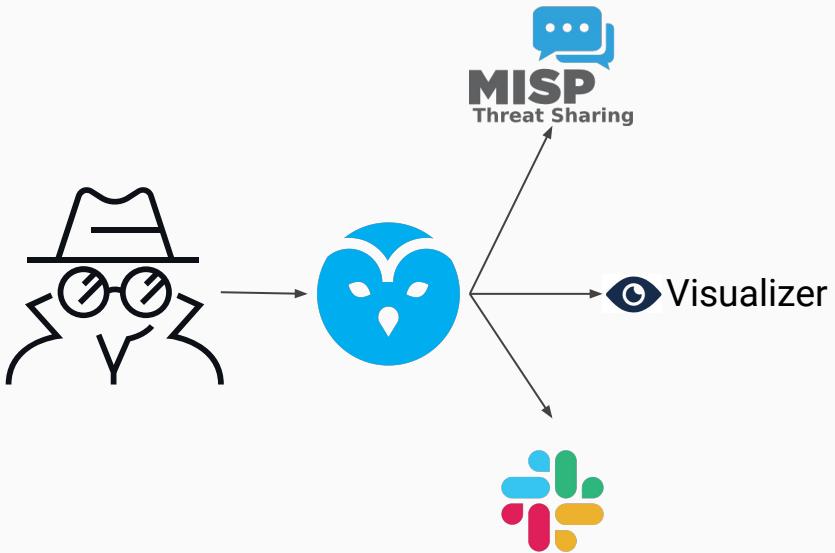
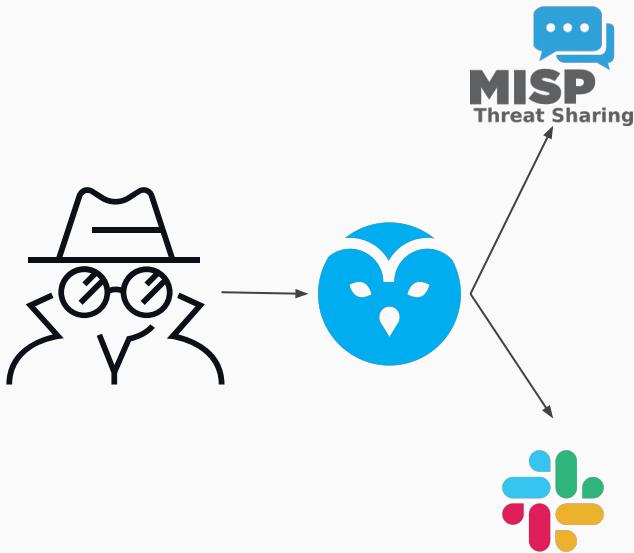
A Threat Intelligence pipeline with IntelOwl (2 / 3)



A Threat Intelligence pipeline with IntelOwl (3 / 3)



A Threat Intelligence pipeline with IntelOwl (3 / 3)



IntelOwl and Google Summer of Code

Since the very beginning of this project we participated in the **Google Summer of Code** under the umbrella of The Honeynet Project! (3 years, 6 successfully completed projects!)

We are participating this year too!

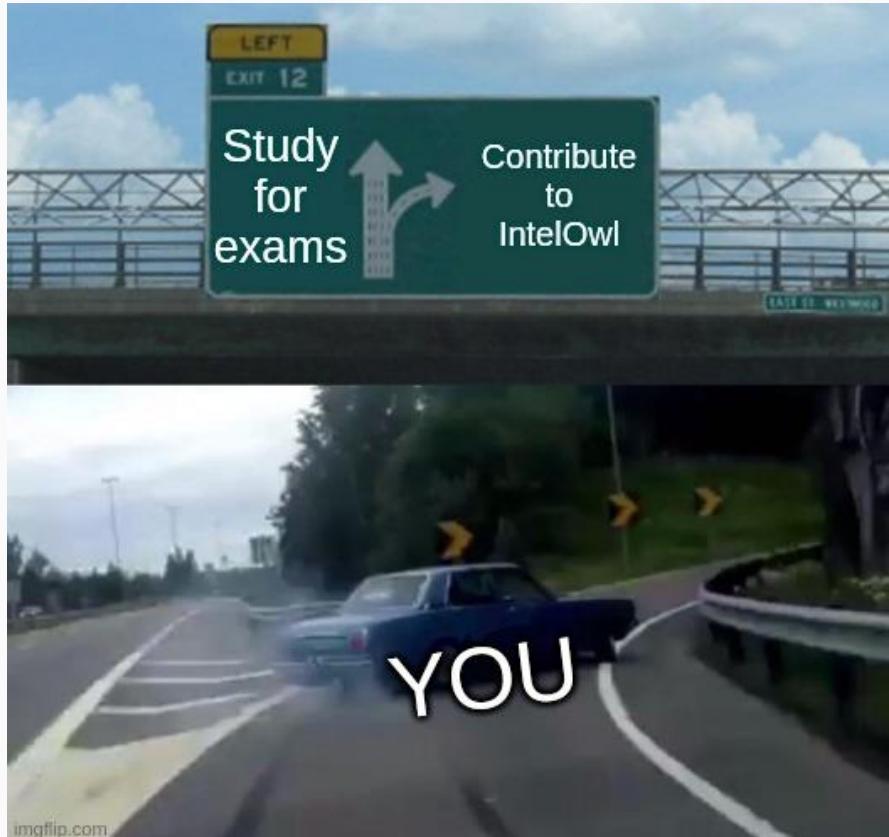


Google Summer of Code

We have selected 2 new contributors this year and they have just started to work for their projects:

- *Abheek Tripathy* is working on creating a new official website for IntelOwl!
- *Shivam Purohit* is working on adding new features like 2FA, Single Sign On with Github, etc

Stay tuned for GSoC 2024!



We are planning to add new critical features in IntelOwl to transform it from a Data Extraction Platform to a complete **Investigation Platform**:



We are planning to add new critical features in IntelOwl to transform it from a Data Extraction Platform to a complete **Investigation Platform**:

- ~~Aggregated and simplified visualization of analyzers results -> IntelOwl v5 released!~~



We are planning to add new critical features in IntelOwl to transform it from a Data Extraction Platform to a complete **Investigation Platform**:

- ~~Aggregated and simplified visualization of analyzers results -> IntelOwl v5 released!~~
- Investigation Framework:
 - Workflows of Analysis (SOAR-like)



We are planning to add new critical features in IntelOwl to transform it from a Data Extraction Platform to a complete **Investigation Platform**:

- ~~Aggregated and simplified visualization of analyzers results -> IntelOwl v5 released!~~
- Investigation Framework:
 - Workflows of Analysis (SOAR-like)
- Support for Cluster Deployments:
 - Docker Swarm
 - Kubernetes
- New Plugins Types:
 - Ingestors
 - Scanners



We are planning to add new critical features in IntelOwl to transform it from a Data Extraction Platform to a complete **Investigation Platform**:

- ~~Aggregated and simplified visualization of analyzers results -> IntelOwl v5 released!~~
- Investigation Framework:
 - Workflows of Analysis (SOAR-like)
- Support for Cluster Deployments:
 - Docker Swarm
 - Kubernetes
- New Plugins Types:
 - Ingestors
 - Scanners
- **Give us YOUR ideas!**
- **Follow us on Twitter, Linkedin and Github!**





Any help is welcome and
valuable!

The icons were collected from: [FlatIcon](#)
Memes were generated with [Imgflip](#)





Thank you for listening!



@matte_lodi @0ssig3no



intelowlproject/IntelOwl

This presentation was reviewed and built together with our awesome team:
Daniele Rosetti and Pietro Delsante

