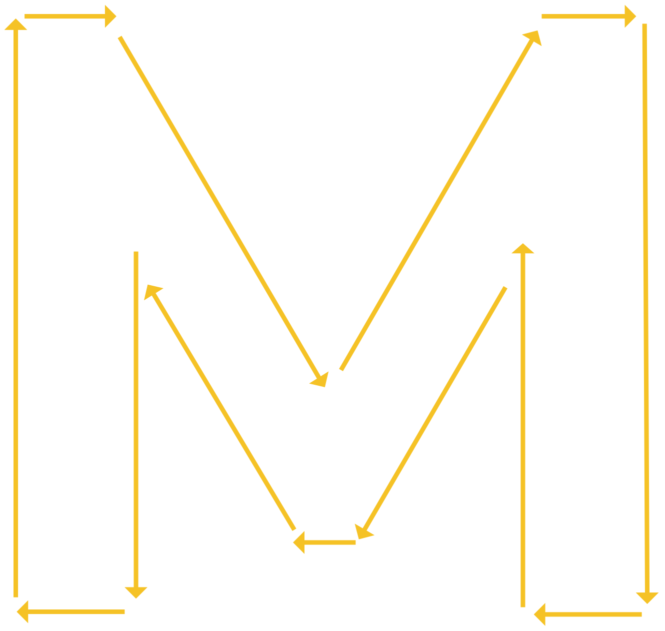
MALTEGO ENTERPRISE MACHINES

A Complete Guide

MALTEGO

Table of Content



Introduction

As a built-in feature in Maltego to automate standard or repetitive investigative steps, Maltego Machines allow users to speed through the process of data collection and allocate more time to analyzing an automatically populated graph.

This guide documents a list of Maltego Machines exclusively available to Maltego Enterprise users. Built according to standard and common workflows used in cybersecurity, cybercriminal, and social media investigations, these Machines allow investigators to quickly gather fundamental data points, thus finishing the groundwork of their investigations with a few clicks of the mouse.

We will continue to develop more Enterprise Machines and will keep you updated on their release by updating this guide as we release them.

For more questions regarding Maltego Machines or suggestions for building future Machines, please reach out to your contact representative at Maltego or write to us at support@maltego.com

Follow us

in Maltego Technologies

@MaltegoHQ

Follow us on Twitter and LinkedIn, and sign up for our email newsletter **newsletter@maltego.com** to gain first-hand updates on the latest Machines.

What Are Maltego Machines?

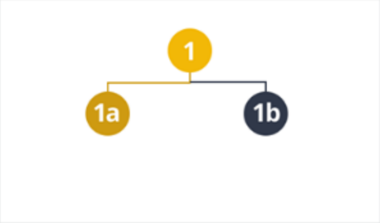
Simply put, Maltego Machines represent the automation of the Transform running process.

Maltego Machines are macros in the Maltego Desktop Client that run multiple Transforms on a data set. These macros are written using the Maltego Scripting Language — a custom scripting language developed to allow any user to create their own Machines.

Depending on the script, Machines can run Transforms in parallel, sequentially, or both. This means users can run multiple Transforms on the same data Entity or run a series of Transforms from one data output to another, or do both at the same time.

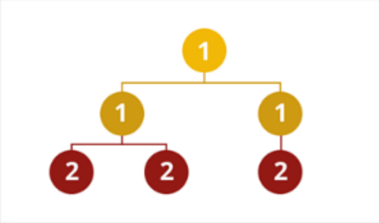
Machines can run transforms in 3 ways:

In Parallel



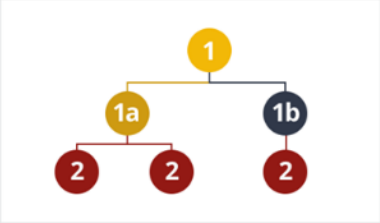
Running multiple Transforms on the **same Entity** at the **same time**

Sequentially



Running Transforms **in a sequence** on **returned Entities** of the previous Transforms

Both



Running Transforms both **in parallel** and **subsequently** on **specified Entities**

Note: Nodes with the same color are results of the same Transform.
The number indicates the order in the Transform sequence of the Machine.

Automate. Save Time.

As the Machine does its work, investigators can use that time for other tasks and preparation. Once the Machine is done, they will see a fully populated graph, the results of which they can begin to analyze.

By standardizing processes and implementing automations, both large investigative teams and individual analysts can allocate their time more efficiently and, thus, establish more streamlined workflows.

Onboard Non-Technical Analysts

Maltego Machines help lower the entry barrier to investigations for non-technical investigators and newcomers to the analyst position. It is common to have a mixture of technical and non-technical investigators with varying degrees of experience working together in analyst teams. By setting up Machines for standardized processes, investigation teams can ensure that all their members, regardless of experience, can conduct important data mapping and link analysis tasks easily and independently.

Three Types of Maltego Machines

1. Out-of-the-Box Machines

Maltego comes with a set of pre-installed Machines that are built with Maltego Standard Transforms. These Machines are free to use for all Maltego users and they query OSINT data to perform tasks like network footprinting.

Maltego Enterprise users also have access to a set of exclusive Enterprise Machines, which we will introduce in this guide.

2. Third-Party Machines

Maltego integrates with a variety of third-party free and paid data sources. Some of these data integrations—RiskIQ PassiveTotal, Farsight DNSDB, etc.—come with Machines created by the integration developers.

Those who have API keys or subscriptions to the data integrations can access these Machines upon installation of the Hub items.

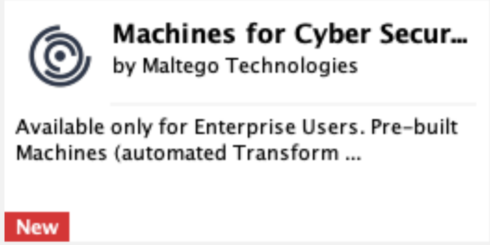
3. Custom Machines

Maltego allows users to create their own Machines. With just a few lines of code, investigators can easily build Machines for their standardized investigative processe

Installing Maltego Enterprise Machines

To start using the Maltego Enterprise Machines, install the Enterprise Machines Hub item as well as all the other Hub items used to create the Machines on your Maltego Desktop Client.

You can find a list of the Hub items used for each Enterprise Machine on the following pages:


Machines for Cyber Secur...
by Maltego Technologies

Available only for Enterprise Users. Pre-built Machines (automated Transform ...

New

Machines for Cyber Secur...
by Maltego Technologies

Available only for Enterprise Users. Pre-built Machines (automated Transform ...

New

Machines for Cyber Secur...
by Maltego Technologies

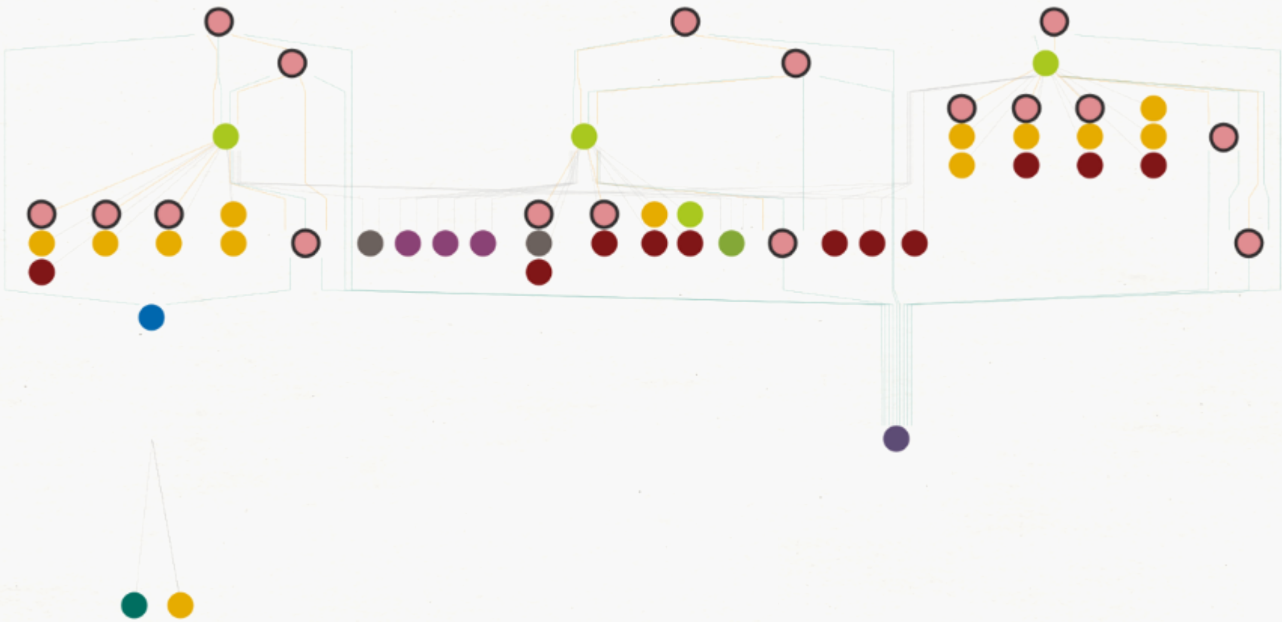
Available only for Enterprise Users. Pre-built Machines (automated Transform ...

New

Maltego Enterprise Machines for Cybersecurity Investigations

Intelligence Gathering L1 – Hashes

[OSINT, Splunk]



The **Intelligence Gathering L1 – Hashes [OSINT, Splunk]** Machine supports basic intelligence gathering on Hash Entities and Splunk validation.

This Machine is essential for SOC teams looking to reduce the amount of time required to enrich information associated with malware hashes—infrastructure information such as C2 domains, URLs, IP addresses, file names, etc.—while at the same time, comparing these findings against their Splunk instance, giving them an edge when fighting malware infections.

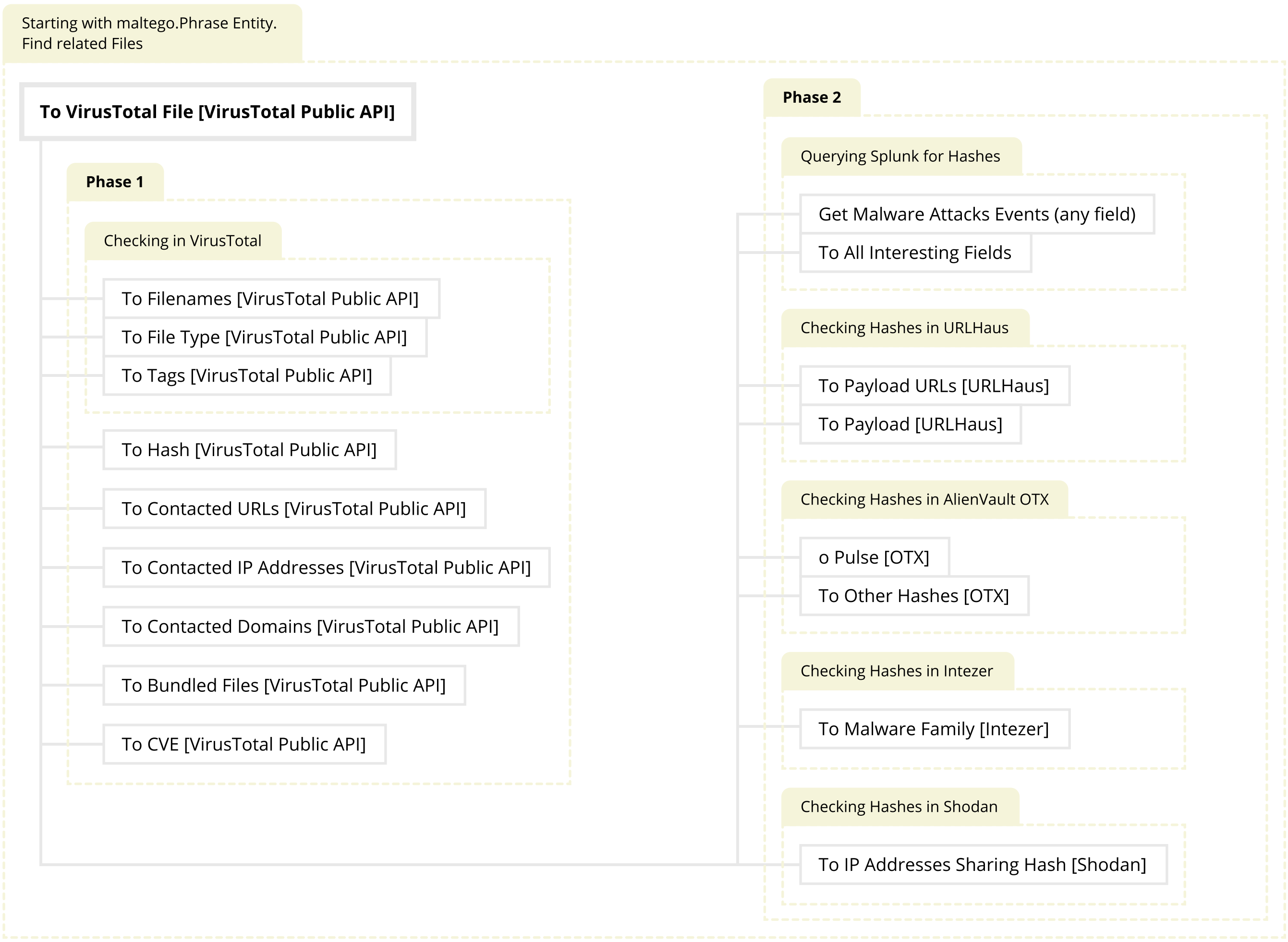
Required Hub Items:

- Abuse.ch URLhaus
- AlienVault OTX
- Intezer Analyze
- Shodan
- Splunk Enterprise Security
- VirusTotal Public API

Intelligence Gathering L1 – Hashes

[OSINT, Splunk]

Transform Sequence



Starting with maltego.Phrase Entity.
Find related Files

To VirusTotal File [VirusTotal Public API]

Phase 1

Checking in VirusTotal

- To Filenames [VirusTotal Public API]
- To File Type [VirusTotal Public API]
- To Tags [VirusTotal Public API]

- To Hash [VirusTotal Public API]
- To Contacted URLs [VirusTotal Public API]
- To Contacted IP Addresses [VirusTotal Public API]
- To Contacted Domains [VirusTotal Public API]
- To Bundled Files [VirusTotal Public API]
- To CVE [VirusTotal Public API]

Phase 2

Querying Splunk for Hashes

- Get Malware Attacks Events (any field)
- To All Interesting Fields

Checking Hashes in URLHaus

- To Payload URLs [URLHaus]
- To Payload [URLHaus]

Checking Hashes in AlienVault OTX

- o Pulse [OTX]
- To Other Hashes [OTX]

Checking Hashes in Intezer

- To Malware Family [Intezer]

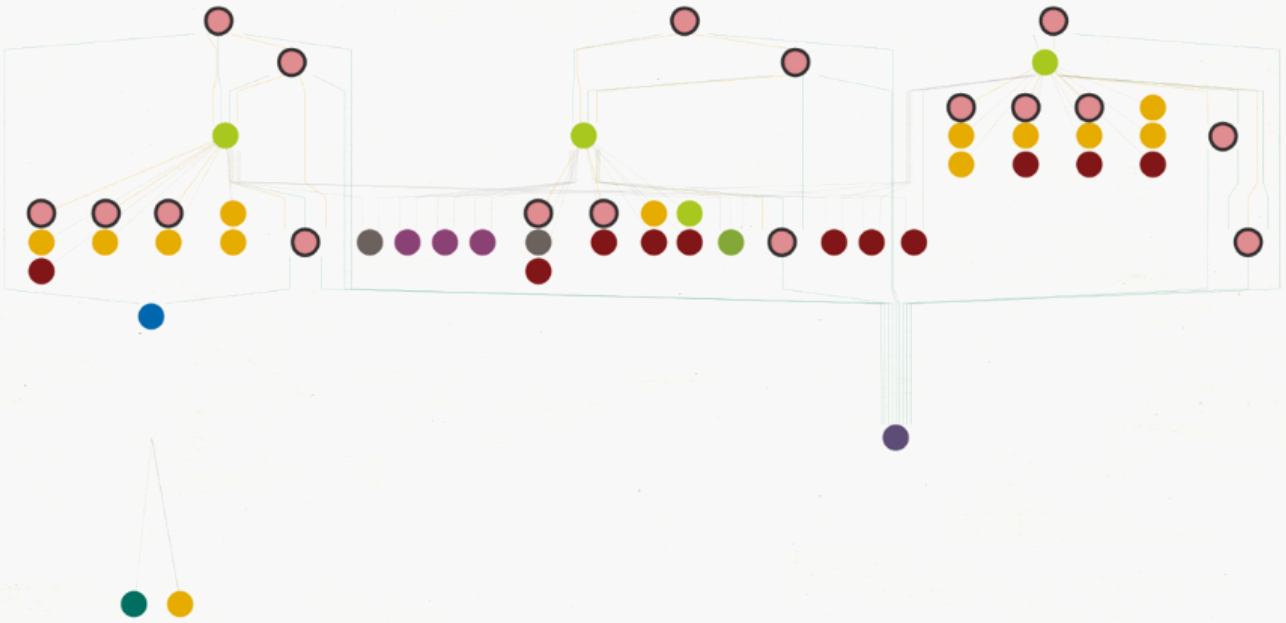
Checking Hashes in Shodan

- To IP Addresses Sharing Hash [Shodan]

Intelligence Gathering L2 – Hashes

[OSINT, Splunk]

While the L1 Machine focuses on providing the first level of information about the hashes and files, this L2 Machine not only checks for infrastructure associated with them, but also checks the data against your Splunk instances.



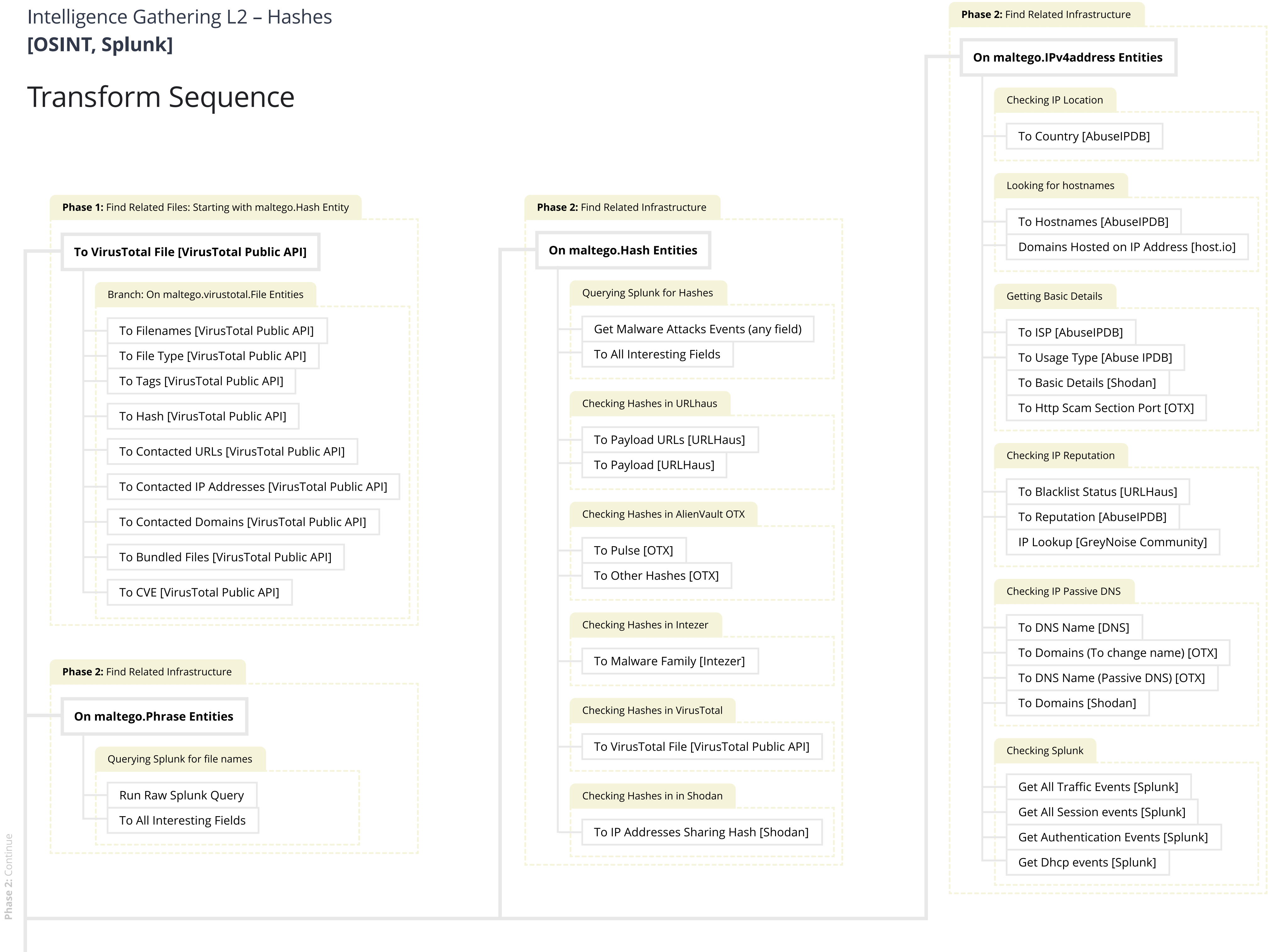
Required Hub Items Additional to those of the L1 Machine:

- AbuseIPDB
- GreyNoise Community
- Host.io
- NIST NVD
- SSL Certificate Transforms
- WhoisXML API

Intelligence Gathering L2 – Hashes

[OSINT, Splunk]

Transform Sequence



Phase 1: Find Related Files: Starting with maltego.Hash Entity

To VirusTotal File [VirusTotal Public API]

Branch: On maltego.virustotal.File Entities

- To Filenames [VirusTotal Public API]
- To File Type [VirusTotal Public API]
- To Tags [VirusTotal Public API]
- To Hash [VirusTotal Public API]
- To Contacted URLs [VirusTotal Public API]
- To Contacted IP Addresses [VirusTotal Public API]
- To Contacted Domains [VirusTotal Public API]
- To Bundled Files [VirusTotal Public API]
- To CVE [VirusTotal Public API]

Phase 2: Find Related Infrastructure

On maltego.Phrase Entities

Querying Splunk for file names

- Run Raw Splunk Query
- To All Interesting Fields

Phase 2: Find Related Infrastructure

On maltego.Hash Entities

Querying Splunk for Hashes

- Get Malware Attacks Events (any field)
- To All Interesting Fields

Checking Hashes in URLhaus

- To Payload URLs [URLHaus]
- To Payload [URLHaus]

Checking Hashes in AlienVault OTX

- To Pulse [OTX]
- To Other Hashes [OTX]

Checking Hashes in Intezer

- To Malware Family [Intezer]

Checking Hashes in VirusTotal

- To VirusTotal File [VirusTotal Public API]

Checking Hashes in in Shodan

- To IP Addresses Sharing Hash [Shodan]

Phase 2: Find Related Infrastructure

On maltego.IPv4address Entities

Checking IP Location

- To Country [AbuseIPDB]

Looking for hostnames

- To Hostnames [AbuseIPDB]
- Domains Hosted on IP Address [host.io]

Getting Basic Details

- To ISP [AbuseIPDB]
- To Usage Type [Abuse IPDB]
- To Basic Details [Shodan]
- To Http Scam Section Port [OTX]

Checking IP Reputation

- To Blacklist Status [URLHaus]
- To Reputation [AbuseIPDB]
- IP Lookup [GreyNoise Community]

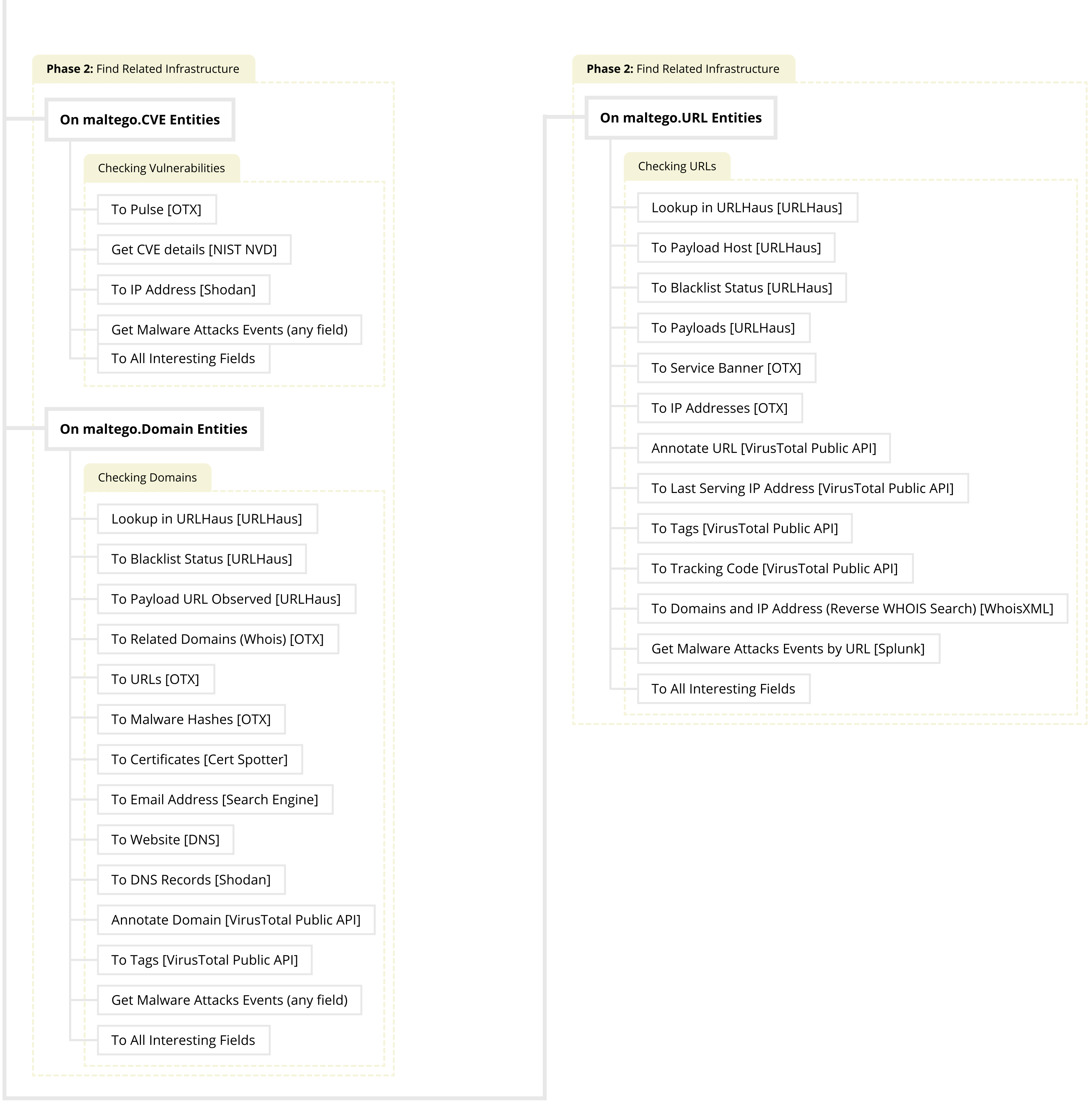
Checking IP Passive DNS

- To DNS Name [DNS]
- To Domains (To change name) [OTX]
- To DNS Name (Passive DNS) [OTX]
- To Domains [Shodan]

Checking Splunk

- Get All Traffic Events [Splunk]
- Get All Session events [Splunk]
- Get Authentication Events [Splunk]
- Get Dhcp events [Splunk]

Phase 2: Continue



Phase 2: Find Related Infrastructure

On maltego.CVE Entities

Checking Vulnerabilities

- To Pulse [OTX]
- Get CVE details [NIST NVD]
- To IP Address [Shodan]
- Get Malware Attacks Events (any field)
- To All Interesting Fields

On maltego.Domain Entities

Checking Domains

- Lookup in URLHaus [URLHaus]
- To Blacklist Status [URLHaus]
- To Payload URL Observed [URLHaus]
- To Related Domains (Whois) [OTX]
- To URLs [OTX]
- To Malware Hashes [OTX]
- To Certificates [Cert Spotter]
- To Email Address [Search Engine]
- To Website [DNS]
- To DNS Records [Shodan]
- Annotate Domain [VirusTotal Public API]
- To Tags [VirusTotal Public API]
- Get Malware Attacks Events (any field)
- To All Interesting Fields

Phase 2: Find Related Infrastructure

On maltego.URL Entities

Checking URLs

- Lookup in URLHaus [URLHaus]
- To Payload Host [URLHaus]
- To Blacklist Status [URLHaus]
- To Payloads [URLHaus]
- To Service Banner [OTX]
- To IP Addresses [OTX]
- Annotate URL [VirusTotal Public API]
- To Last Serving IP Address [VirusTotal Public API]
- To Tags [VirusTotal Public API]
- To Tracking Code [VirusTotal Public API]
- To Domains and IP Address (Reverse WHOIS Search) [WhoisXML]
- Get Malware Attacks Events by URL [Splunk]
- To All Interesting Fields

Maltego Enterprise Machines for Cybercrime Investigations

Identify Relevant Threat Actors

[Intel 471]

The **Identify Relevant Threat Actors [Intel 471]** Machine queries the Intel 471 underground dataset to identify threat actors who have authored posts mentioning specific keywords.

This Machine is of great help to threat intelligence analysts, government investigators, journalists, and security researchers looking to gain additional insights from conversations taking place on dark web forums.

Required Hub Item:

- Intel 471(Enterprise)

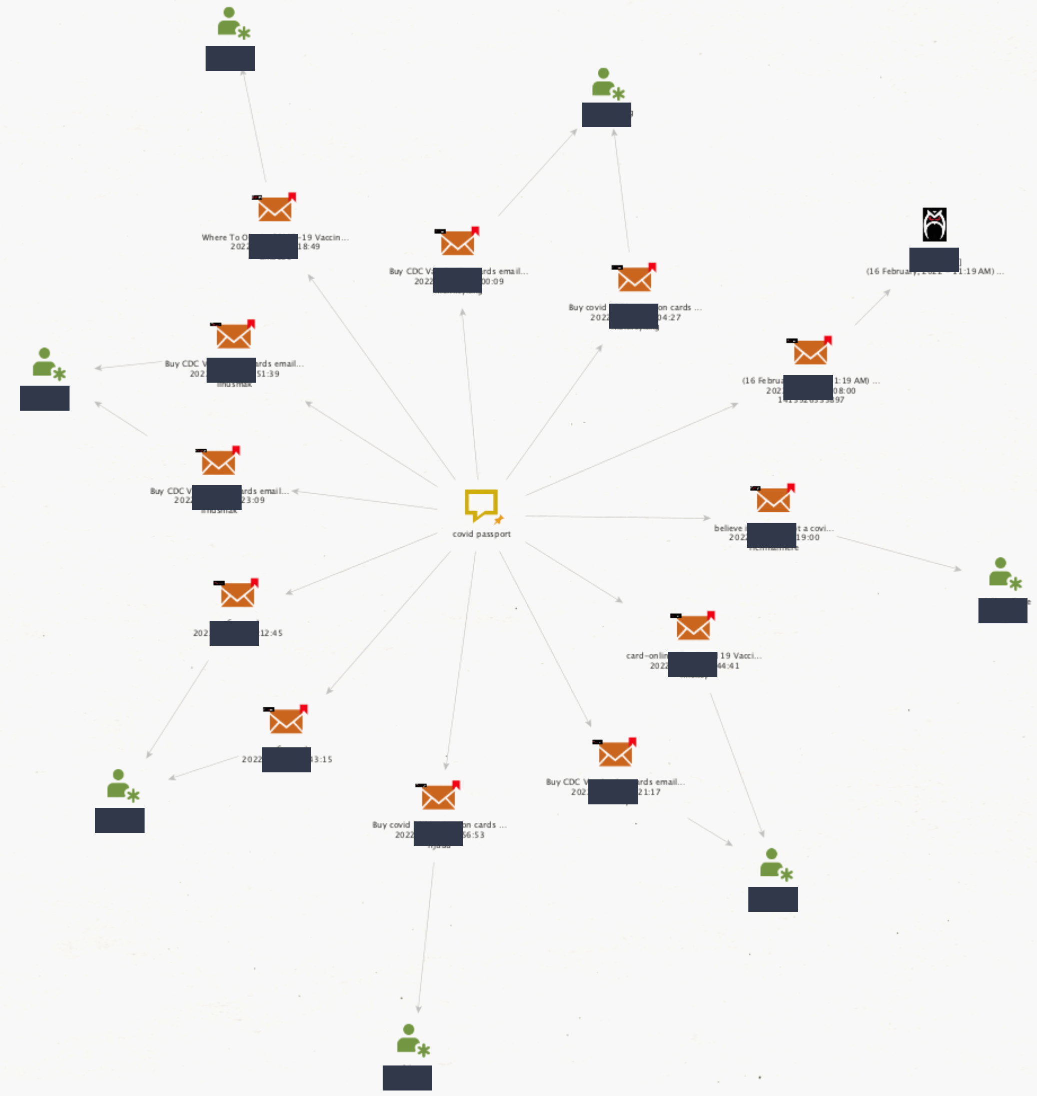
INTEL471

Transform Sequence

Starting with maltego.Phrase Entity

[Intel 471] Phrase to Post

[Intel 471] Phrase to Alias



Identify Relevant Forum Threads

[Intel 471]

The Identify Relevant Forum Threads [Intel 471] Machine identifies forum threads mentioning a keyword as well as the corresponding thread authors.

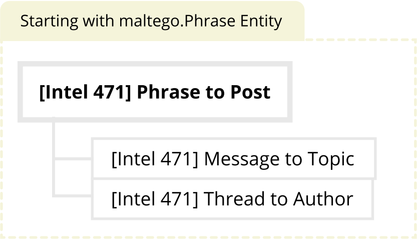
This Machine identifies dark web forum thread topics as well as the threat actors behind the conversations.

Required Hub Item:

- Intel 471(Enterprise)

INTEL471

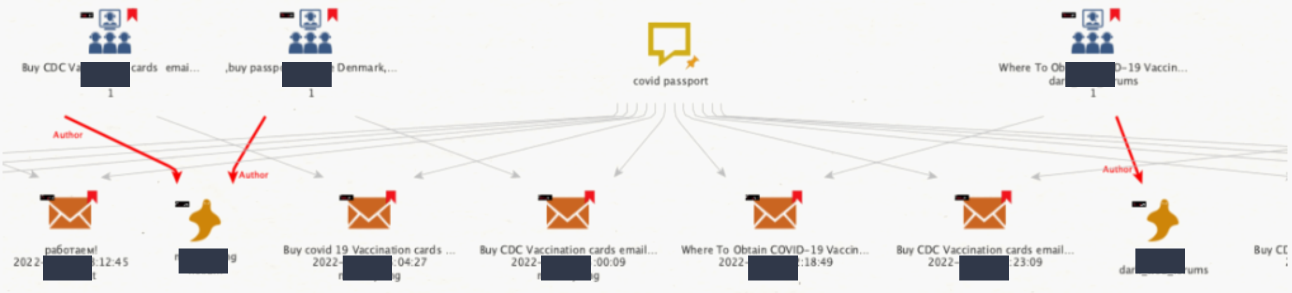
Transform Sequence


Starting with maltego.Phrase Entity

[Intel 471] Phrase to Post

[Intel 471] Message to Topic

[Intel 471] Thread to Author



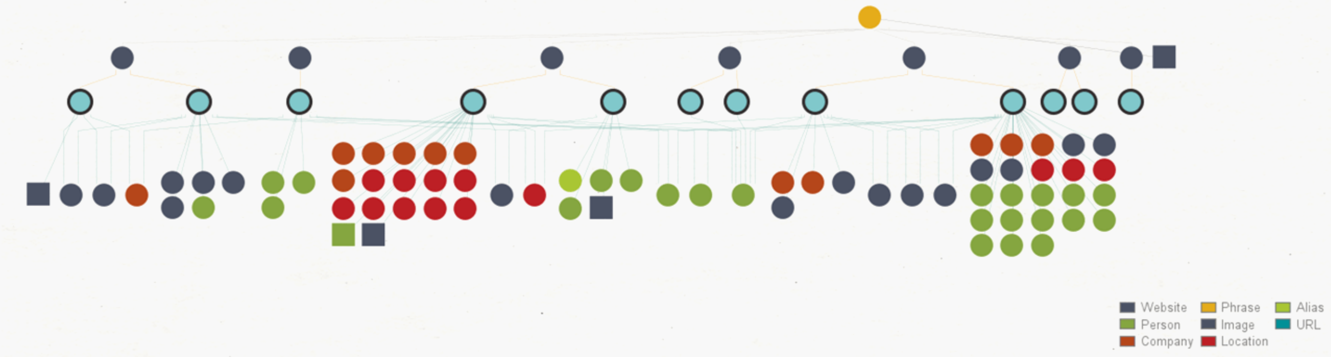
Buy CDC Va [redacted] cards emai...
1
,buy passp [redacted] Denmark,...
1
covid passport
Where To Ob [redacted] D-19 Vaccin...
dar [redacted] ums
1
Author
Author
Author
работаем!
2022- [redacted] :12:45
[redacted]
Buy covid 19 Vaccination cards ...
2022- [redacted] :04:27
Buy CDC Vaccination cards email...
2022- [redacted] :00:09
Where To Obtain COVID-19 Vaccin...
2022- [redacted] :18:49
Buy CDC Vaccination cards email...
2022- [redacted] :23:09
[redacted]
dar ums
Buy CI

Maltego Enterprise Machines for Social Media & Person-of-Interest Investigations

Basic Digital Footprint
[OSINT]

The **Basic Digital Footprint [OSINT]** Machine maps the online footprint of a person's name or alias. This is a perfect Machine to gain a basic, yet comprehensive overview of where a person's name or alias has appeared on the internet, as well as what images, locations, and other individuals or organizations are associated with said name or alias.

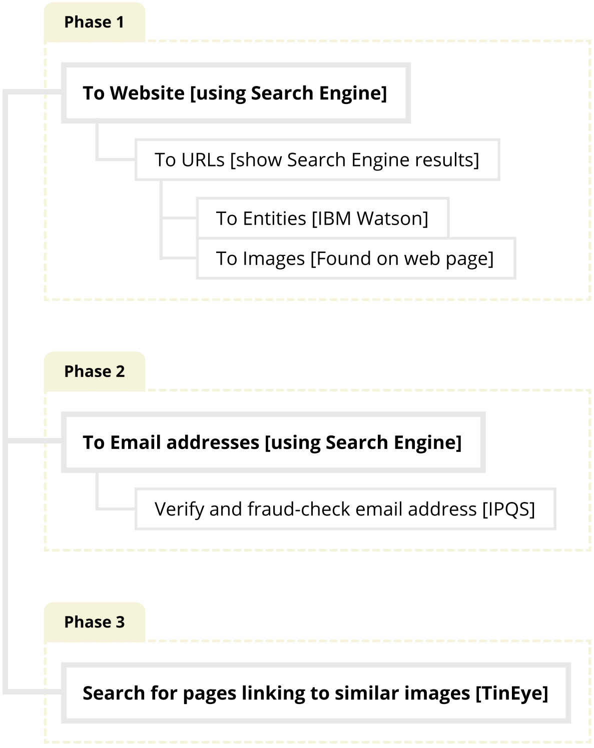
The Machine is available for free and requires no additional API keys for the Hub items involved. During the data gathering process, the Machine will prompt you to examine the relevance of the query results to ensure high relevancy of the output delivery.



Required Hub Item:

- Maltego Standard Transforms
- TinEye

Transform Sequence



Phase 1

To Website [using Search Engine]

To URLs [show Search Engine results]

To Entities [IBM Watson]

To Images [Found on web page]

Phase 2

To Email addresses [using Search Engine]

Verify and fraud-check email address [IPQS]

Phase 3

Search for pages linking to similar images [TinEye]

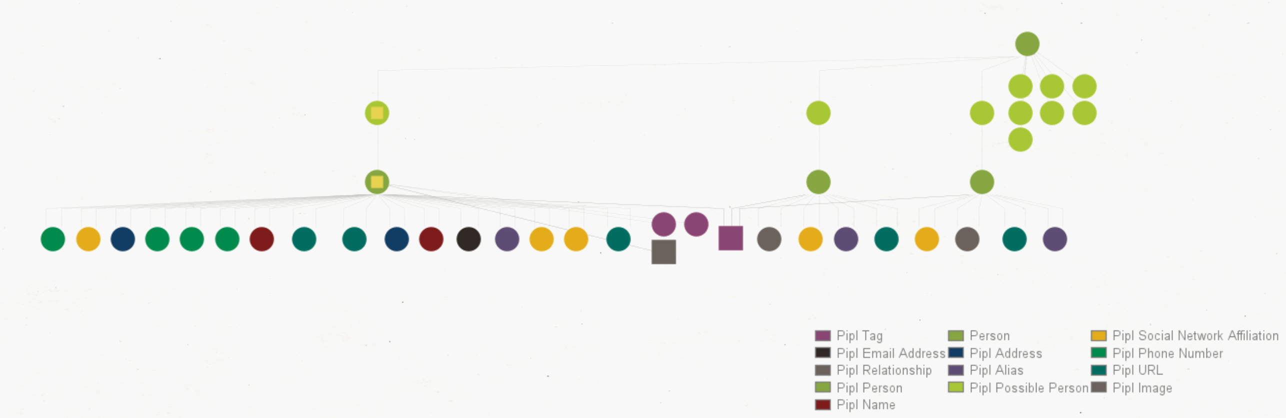
Full Identity Footprint

[Pipl]

The **Full Identity Footprint [Pipl]** Machines are useful for zooming in on a person’s real-life information and quickly building a profile of your person-of-interest.

Querying the Pipl identity database, this Machine retrieves a person’s current and historical information:

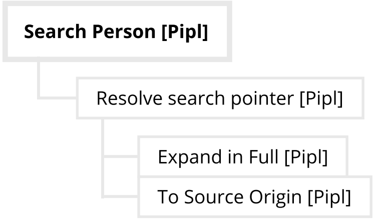
- Full Name
- Image(s)
- Physical Address(es)
- Email Address(es)
- Phone Number(s)
- Website(s) & Social Media Handle(s)
- Education and Career History
- Associate(s) & Relation(s)
- Hobbies and Interests



Required Hub Item:

- Pipl

Transform Sequence



Search Person [Pipl]

Resolve search pointer [Pipl]

Expand in Full [Pipl]

To Source Origin [Pipl]

Deep Social Media Footprint

[ShadowDragon Social Net]

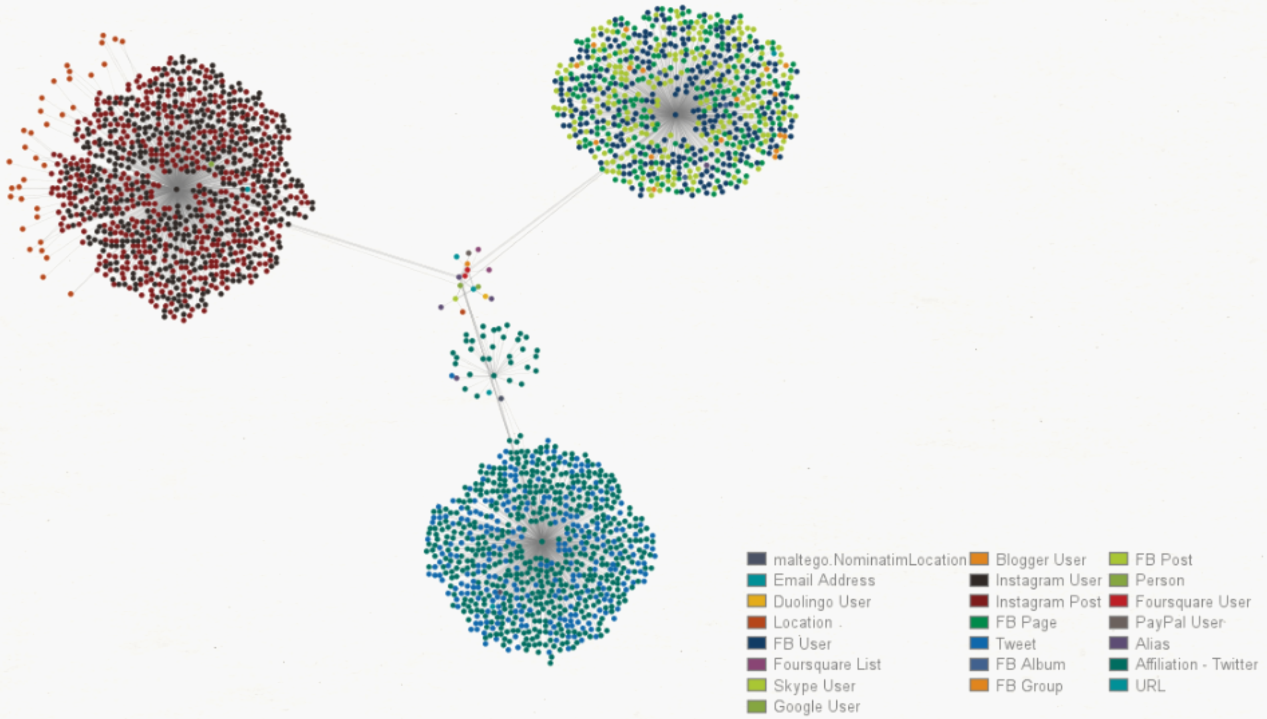
The Deep Social Media Footprint [ShadowDragon SocialNet] Machine maps the social media footprint of a person's name or alias. The Machine focuses on the person's associated network of connections on Instagram and Twitter.

This Machine gives an extensive insight into the following social aspects of a person-of-interest:

- Whose content they consume via Twitter following
- Where they visit via Instagram location sharing

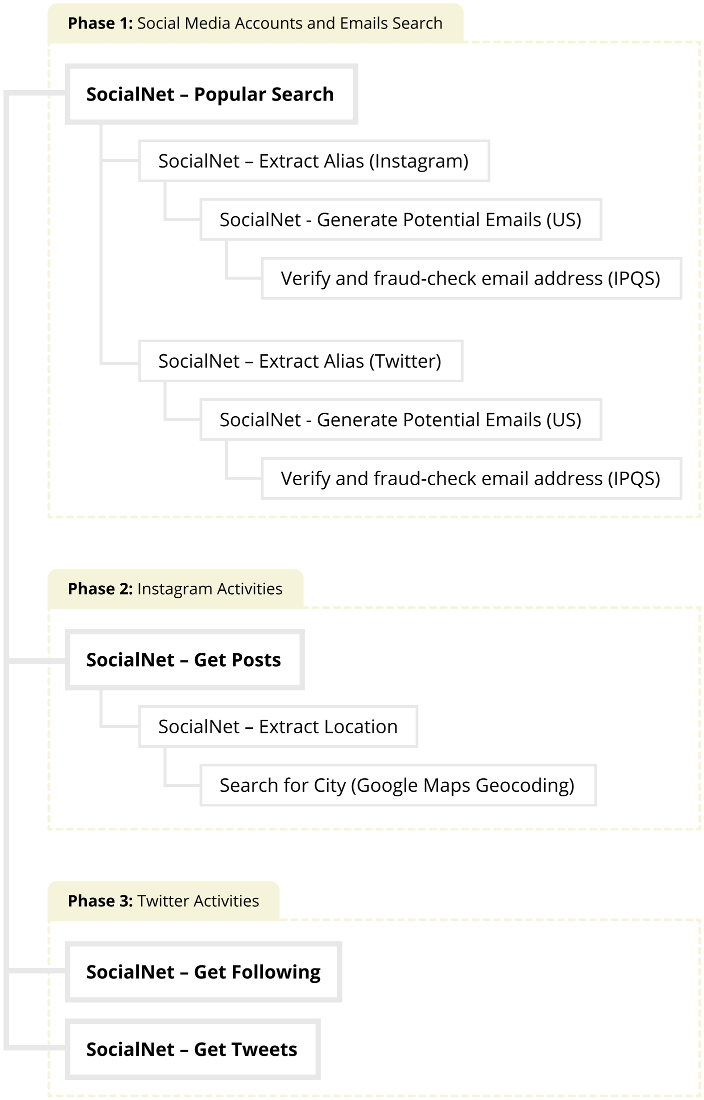
Required Hub Item:

- ShadowDragon's SocialNet
- Maltego Standard Transforms
- Google Maps Geocoding



Deep Social Media Footprint
[ShadowDragon, SocialNet]

Transform Sequence



Phase 1: Social Media Accounts and Emails Search

- **SocialNet – Popular Search**
  - SocialNet – Extract Alias (Instagram)
    - SocialNet - Generate Potential Emails (US)
      - Verify and fraud-check email address (IPQS)
  - SocialNet – Extract Alias (Twitter)
    - SocialNet - Generate Potential Emails (US)
      - Verify and fraud-check email address (IPQS)

Phase 2: Instagram Activities

- **SocialNet – Get Posts**
  - SocialNet – Extract Location
    - Search for City (Google Maps Geocoding)

Phase 3: Twitter Activities

- **SocialNet – Get Following**
- **SocialNet – Get Tweets**

MALTEGO

Maltego is a comprehensive tool for graphical link analyses that offers real-time data mining and information gathering, as well as the representation of this information on a node-based graph, making patterns and multiple order connections between said information easily identifiable. With Maltego, you can easily mine data from dispersed sources, automatically merge matching information in one graph, and visually map it to explore your data landscape. Maltego offers the ability to easily connect data and functionalities from diverse sources using Transforms. Via the Transform Hub, you can connect data from over 30 data partners, a variety of public sources (OSINT) as well as your own data. Our different Desktop Client versions, data sources, and server solutions enable you to tailor Maltego to your specific needs in terms of data access, functionalities, and security requirements.

For more questions regarding Maltego Machines or suggestions for building future Machines, please reach out to your contact representative at Maltego or write us at **support@maltego.com**