



Transforms for Maltego

INSTALLATION AND SUMMARY OF TRANSFORMS

TABLE OF CONTENTS

Introduction.....	3
Installation	4
Install Step 1: Transform Hub	4
Install Step 2: Recorded Future API Token	5
Configuration Tips	5
Transform Slider	6
Collections	6
Filtering the RF Documents to Retrieve.....	6
Maltego Entities.....	9
Maltego Transforms	11
Entity to Intel Summary.....	11
Entity to RF Documents	11
Entity to Analyst Note.....	12
Entity to Attack Vector	13
Entity to Malware.....	13
Entity to Malware Category	14
Entity to Malware Signature.....	14
Entity to Vulnerability.....	15
Entity to Operation	15
Entity to Domain.....	15
Entity to Email	16
Entity to Filename	16
Entity to Hash.....	17
Entity to IP Address.....	17
Entity to Registry Key	18
Entity to URL	18
Entity to Organization	18
Entity to AS Number	19
Entity to Company	19
Phrase to Threat Intel Entities.....	19
Maltego Machines	20
Getting Support	21
Appendix A: Transform List	22

INTRODUCTION

The documentation describes the integration between Recorded Future and Maltego.

The integration consists of a set of Entities, Transforms, and Machines. This integration is available to customers of Recorded Future, and is provided by Recorded Future and Malformity Labs.



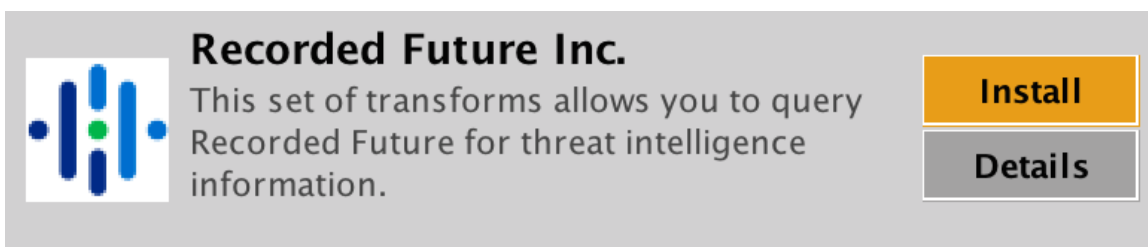
INSTALLATION

The installation has two steps:

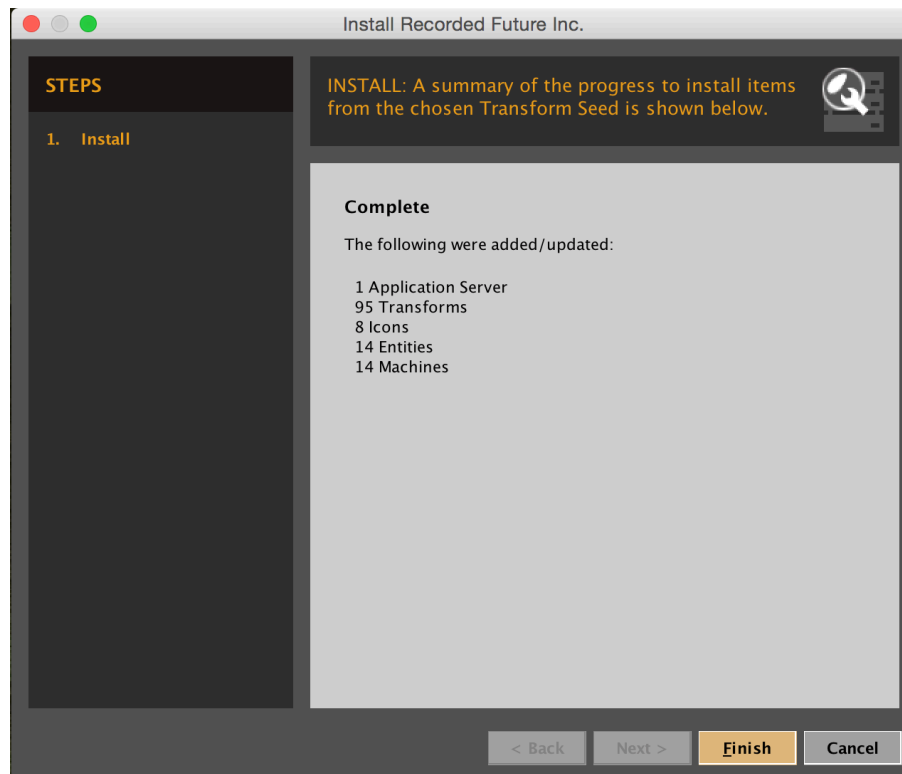
1. Install the Entities, Transforms, and Machines
2. Enable the transforms with your Recorded Future API token

INSTALL STEP 1: TRANSFORM HUB

You can install the Recorded Future integration through the Maltego Transform Hub. In the Hub, look for the Recorded Future transforms tile. Hover over the tile and click the Install button.



The entities, transforms, and machines are automatically installed.



INSTALL STEP 2: RECORDED FUTURE API TOKEN

Each transform must be linked to your Recorded Future API token. You will be prompted to enter your Recorded Future API token when installing from the transform hub.

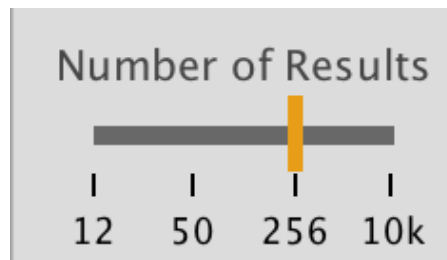
To create or find your API token, log in to Recorded Future and navigate to **User Settings**, located in the upper right corner of the interface. Find your token under **API Access**. Note that API tokens are case sensitive.

More details about managing Recorded Future API Tokens is available on this support page: <https://support.recordedfuture.com/hc/en-us/articles/115004179227-Managing-API-tokens>. In addition, you can contact support @ recordedfuture.com if you need help with your API token.

CONFIGURATION TIPS

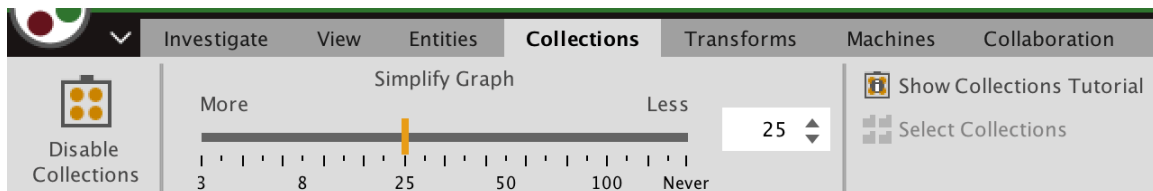
TRANSFORM SLIDER

The transform slider can be used to control how many entities will be returned for any given entity. The slider values will depend on your version of Maltego, but each respective slider will contain designated limits you can select.



COLLECTIONS

Collections can be used to simplify your graph as it grows. Turning on collections will automatically collapse leaf nodes of the same type within your graph. You can also set the point at which you want collections to take effect.



On the graph, collections will look similar to the example below, which contains a collection of RF Document entities.



FILTERING THE RF DOCUMENTS TO RETRIEVE

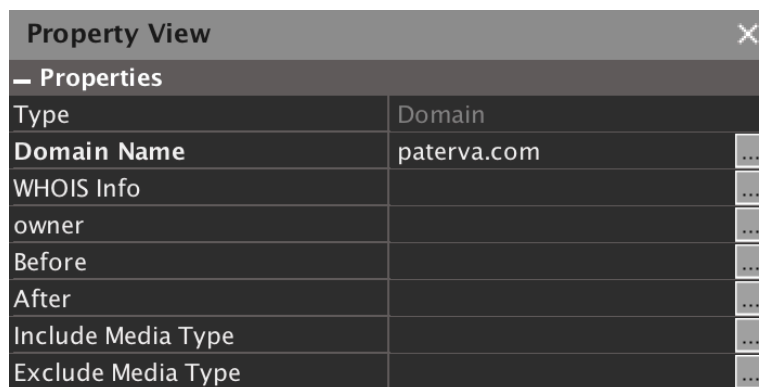
When applying these transforms to cyber indicators or observables, generally some observables will return a few matches, and others will match nothing – but a few will have many more matches than can be easily investigated in a Maltego graph.

In these cases, you can navigate from Maltego into the Recorded Future web application to analyze the related events.

You can also filter the set of RF Documents retrieved by the transforms, using these properties:

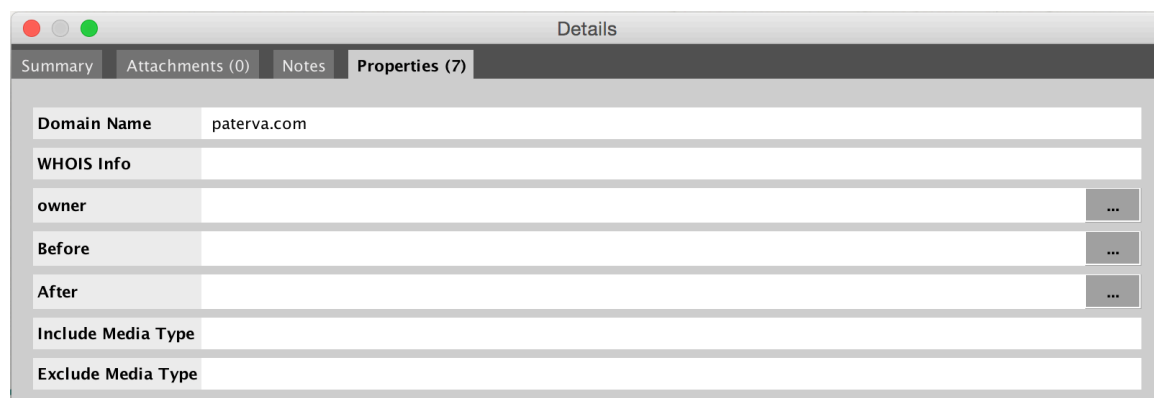
- Only documents published on or *Before* a date in YYYY-MM-DD format
- Only documents published on or *After* a specific date in YYYY-MM-DD format
- Only documents from *Include Media Types*, a comma-separated list
- Omit documents from *Exclude Media Types*, a comma-separated list

To edit these filter properties, you can either directly edit the values in the property view or you can double-click on an Entity and select the *Properties* tab.



The Property View dialog box is a small window with a title bar that says "Property View" and a close button (X). It contains a table with two columns: "Type" and "Domain". The "Domain" column has a dropdown menu with "paterva.com" selected. The "Type" column has several rows: "Domain Name", "WHOIS Info", "owner", "Before", "After", "Include Media Type", and "Exclude Media Type". Each row has a dropdown menu to its right, indicated by three dots.

Type	Domain
Domain Name	paterva.com
WHOIS Info	
owner	
Before	
After	
Include Media Type	
Exclude Media Type	



The Details window is a larger application window with a title bar that says "Details". It has a tabbed interface with tabs for "Summary", "Attachments (0)", "Notes", and "Properties (7)". The "Properties (7)" tab is selected. It contains a table with two columns: "Property Name" and "Value". The "Property Name" column has several rows: "Domain Name", "WHOIS Info", "owner", "Before", "After", "Include Media Type", and "Exclude Media Type". The "Value" column has a text input field for "Domain Name" containing "paterva.com", and empty text input fields for the other properties. Each row has a dropdown menu to its right, indicated by three dots.

Property Name	Value
Domain Name	paterva.com
WHOIS Info	
owner	
Before	
After	
Include Media Type	
Exclude Media Type	

Note: Media Type is the same as “Source Types” in the Advanced Query Panel in Recorded Future; more information about them is available on this support page: <https://support.recordedfuture.com/hc/en-us/articles/115001359907-Source-Types>.

MALTEGO ENTITIES

The integration uses default Maltego Entities and Malformity Labs Entities to represent observables, for compatibility with other transform sets. Recorded Future also defines several entity types that are not common Maltego or Malformity Labs entities.

These Entities are supported:

Maltego Entities

- Alias
- AS Number
- Company
- Domain
- Email Address
- Hash
- IPv4 Address
- NSRecord
- MXRecord
- Organization
- Phrase
- URL

Malformity Labs Entities

- Filename
- Mutex
- Registry Entry – returned values are registry keys

Recorded Future Entities

- Analyst Note – Research notes written by Recorded Future’s Insikt Group
- Attack Vector – Cyber attack vector (e.g., cross site scripting, DDOS, Phishing)
- Malware – Common malware street names (e.g., Locky, Wcry, Mirai)
- Malware Category – Common categories of malware (e.g., Ransomware, Adware, Trojan)
- Malware Signature – detection signature names, usually anti-virus
- Operation – hacktivist operations and APT campaigns

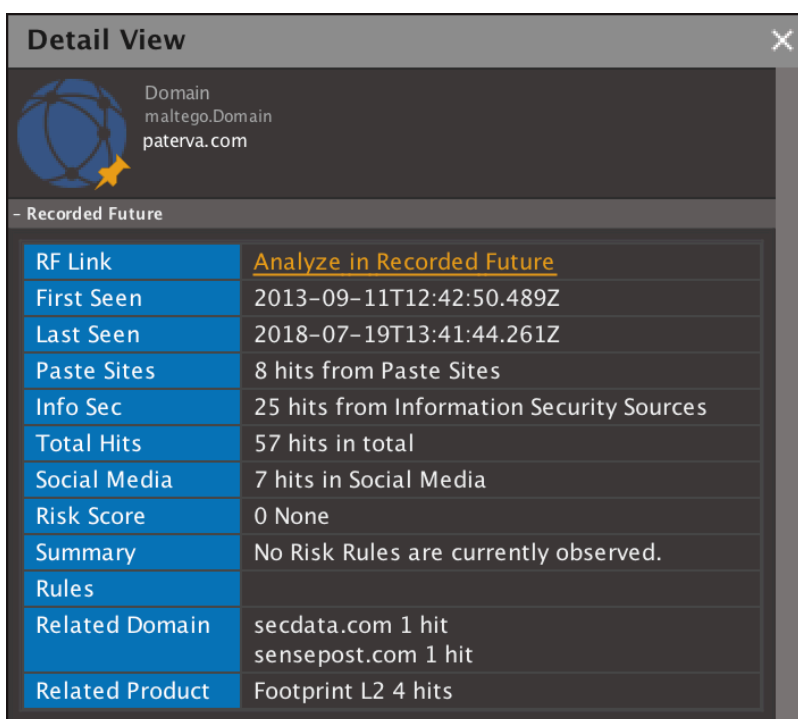
- Recorded Future Doc – a web document analyzed by Recorded Future
- Vulnerability – NIST CVE numbers and vendor-specific advisory numbers

MALTEGO TRANSFORMS

Each supported Entity has a number of transforms that can be run to search and return related data or entities. They are organized here by output type and a full list of transforms present in the transform set is available in Appendix A.

ENTITY TO INTEL SUMMARY

These transforms retrieve summary metrics about available information in Recorded Future, and correspond with information available on a Recorded Future Intelligence card. The metric data is available in the detail pane of the entity and includes the information in the screenshot below.



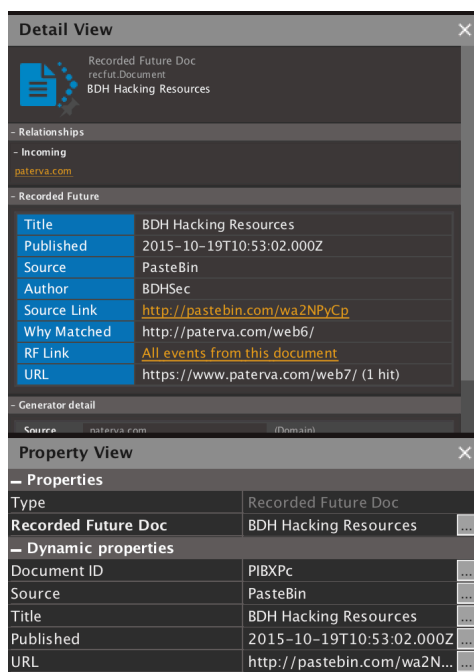
The screenshot shows the 'Detail View' window in Maltego. At the top, it displays the domain 'maltego.Domain' and 'paterva.com' next to a globe icon. Below this, a section titled '- Recorded Future' contains a table of metrics. The 'RF Link' is highlighted with a yellow link text 'Analyze in Recorded Future'. Other metrics include 'First Seen', 'Last Seen', 'Paste Sites', 'Info Sec', 'Total Hits', 'Social Media', 'Risk Score', 'Summary', 'Rules', 'Related Domain', and 'Related Product'.

Domain	
maltego.Domain	paterva.com
- Recorded Future	
RF Link	Analyze in Recorded Future
First Seen	2013-09-11T12:42:50.489Z
Last Seen	2018-07-19T13:41:44.261Z
Paste Sites	8 hits from Paste Sites
Info Sec	25 hits from Information Security Sources
Total Hits	57 hits in total
Social Media	7 hits in Social Media
Risk Score	0 None
Summary	No Risk Rules are currently observed.
Rules	
Related Domain	secdata.com 1 hit sensepost.com 1 hit
Related Product	Footprint L2 4 hits

The “RF Link” is clickable from within Maltego and will open the relevant Recorded Future link in your browser.

ENTITY TO RF DOCUMENTS

These transforms expand your graph with **RF Document** entities. Each web document returned has reported events involving the input Entity. This data can be viewed in the detail and property views for the entity.



In the **Details** view, you can review information about the web documents:

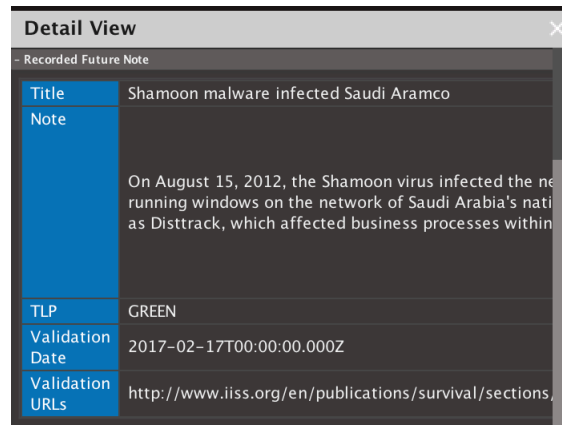
- Title
- Source name, publication date, and original document URL
- Fragments: excerpts from the document which refer to the Entity
- Backtrack link to analyze matching events in Recorded Future

ENTITY TO ANALYST NOTE

These transforms expand your graph with **Analyst Note** entities. Each entity returned has long form written text regarding the entity in question. This data can be viewed in the detail and property views for the entity.



The Detail View for this entity includes the title of the document, as well as an analyst provided note or comment. In addition, the TLP category, date and supporting URLs are also provided.

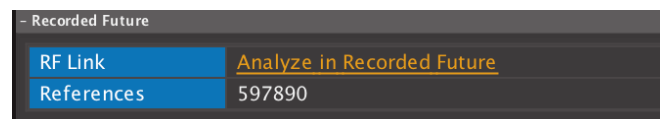


ENTITY TO ATTACK VECTOR

These transforms expand your graph with **Attack Vector** entities. Each entity returned has reported events involving the input entity. This data can be viewed in the detail and property views for the entity.



The Detail View for this entity includes a link to investigate the entity within Recorded Future, as well as a count of the number of references within the system for the entity in question.



ENTITY TO MALWARE

These transforms expand your graph with **Malware** entities. Each entity returned has reported events involving the input entity.



ENTITY TO MALWARE CATEGORY

These transforms expand your graph with **Malware Category** entities. Each entity returned has reported events involving the input entity.



ENTITY TO MALWARE SIGNATURE

These transforms expand your graph with **Malware Signature** entities. Each entity returned has reported events involving the input entity. This data can be viewed in the detail and property views for the entity.



The Detail View for this entity includes a link to investigate the entity within Recorded Future, as well as a count of the number of references within the system for the entity in question.

- Recorded Future	
RF Link	Analyze in Recorded Future
References	1259455

ENTITY TO VULNERABILITY

These transforms expand your graph with **Vulnerability** entities. Each entity returned has reported events involving the input entity.



ENTITY TO OPERATION

These transforms expand your graph with **Operation** entities. Each entity returned has reported events involving the input entity.



ENTITY TO DOMAIN

These transforms expand your graph with **Domain** entities. Each entity contains a variety of descriptive information about the entity. This data can be viewed in the detail and property views for the entity.



The Detail View for this entity includes a link to analyze the entity in Recorded Future, relevant dates and counts, a risk score and summary, as well as related hashes and domains.

Detail View	
- Recorded Future	
RF Link	Analyze in Recorded Future
First Seen	2017-01-23T23:31:37.023Z
Last Seen	2018-09-11T02:48:19.018Z
Info Sec	246 hits from Information Security Sources
Total Hits	246 hits in total
Risk Score	0 None
Summary	No Risk Rules are currently observed.
Rules	
Related Hash	03ce2c4ab77e2d3c2d5cf1889037d886f54c7d9352d6631 hit

ENTITY TO EMAIL

These transforms expand your graph with **Email Address** entities. Each entity returned has reported events involving the input entity.



ENTITY TO FILENAME

These transforms expand your graph with **Filename** entities. Each entity returned has reported events involving the input entity. This data can be viewed in the detail and property views for the entity.



The Detail View for this entity includes a link to investigate the entity within Recorded Future, as well as a count of the number of references within the system for the entity in question.

- Recorded Future	
RF Link	Analyze in Recorded Future
References	162040

ENTITY TO HASH

These transforms expand your graph with **Hash** entities. Each entity contains a variety of descriptive information about the entity. This data can be viewed in the detail and property views for the entity.



The Detail View for this entity includes a link to analyze the entity in Recorded Future, relevant dates and counts, a risk score and summary, as well as related hashes and domains.

Detail View	
- Recorded Future	
RF Link	Analyze in Recorded Future
Algorithm	MD5
First Seen	2017-08-14T06:27:59.983Z
Last Seen	2018-09-11T02:48:19.018Z
Info Sec	10 hits from Information Security Sources
Total Hits	10 hits in total
Risk Score	65 Malicious
Summary	1 of 10 Risk Rules currently observed.
Rules	Positive Malware Verdict
Related Hash	0f343b0931126a20f133d67c2b018a3b 10 hits d0220b77b9370e8493a519d15d948712 10 hits

ENTITY TO IP ADDRESS

These transforms expand your graph with **IP Address** entities. Each entity returned has reported events involving the input entity.

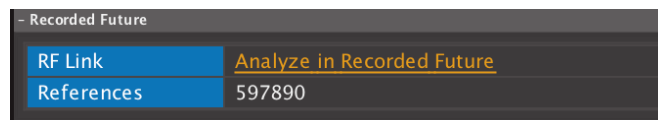


ENTITY TO REGISTRY KEY

These transforms expand your graph with **Registry Key** entities. Each entity returned has reported events involving the input entity. This data can be viewed in the detail and property views for the entity.



The Detail View for this entity includes a link to investigate the entity within Recorded Future, as well as a count of the number of references within the system for the entity in question.



ENTITY TO URL

These transforms expand your graph with **URL** entities. Each entity returned has reported events involving the input entity.



ENTITY TO ORGANIZATION

These transforms expand your graph with **Organization** entities. Each entity returned has reported events involving the input entity.



ENTITY TO AS NUMBER

These transforms expand your graph with **AS Number** entities. Each entity returned has reported events involving the input entity.



ENTITY TO COMPANY

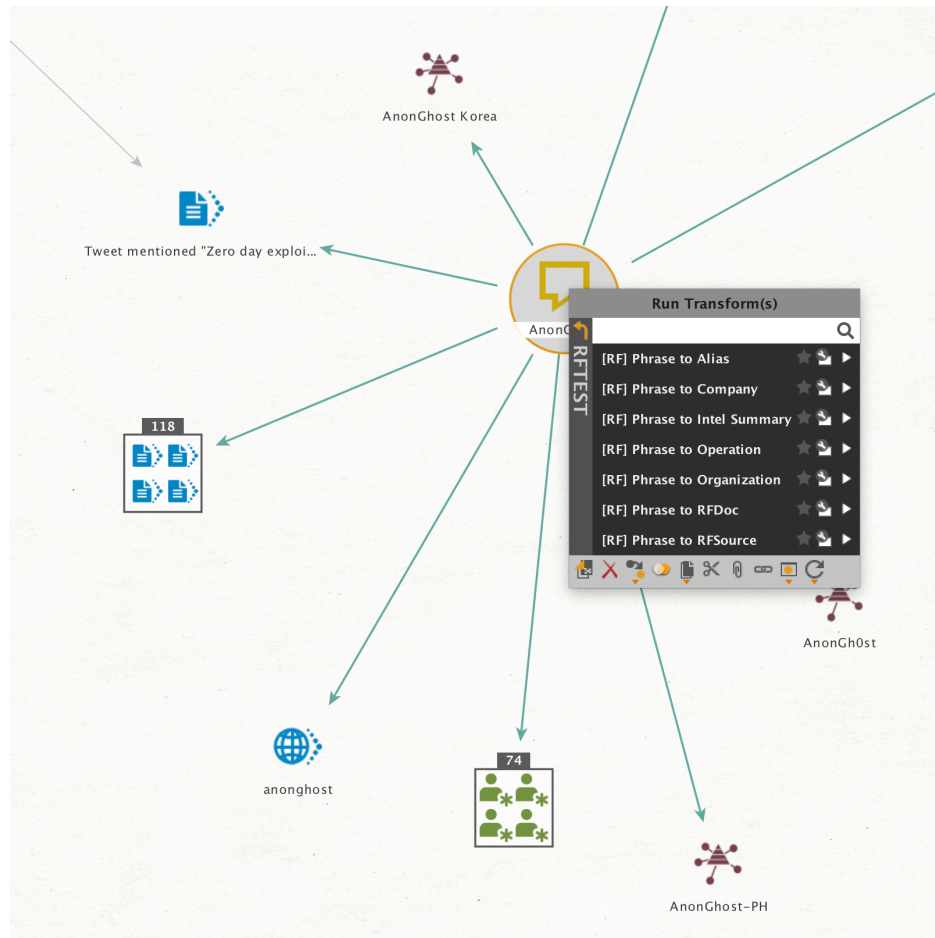
These transforms expand your graph with **Company** entities. Each entity returned has reported events involving the input entity.



PHRASE TO THREAT INTEL ENTITIES

When you start an investigation from a set of indicators or observables, the "mapping" from your initial data to Recorded Future entities is straightforward. Simple paste the entity text into Maltego, correct the automatically detected entity types if necessary, and begin running transforms. Maltego will recognize many entity types using regular expressions.

When your investigation starts with a threat actor or target organization, you begin by using the Maltego *Phrase* entity to map the threat actor or target to a Recorded Future entity. This mapping will resolve variations in spelling and naming (e.g. *AnonGhost* vs. *AnonGh0st*.)

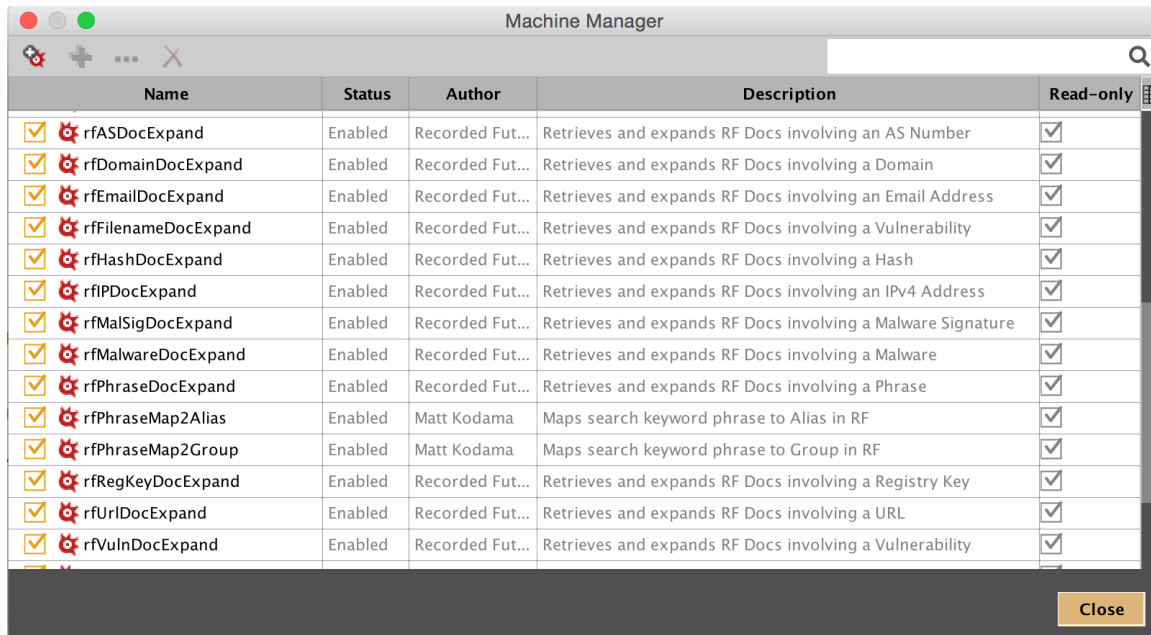


You can map the input *Phrase* to an Alias (representing a person, Social Media profile, or forum username), Company, Operation, or Organization. Organizations can represent both threat actor groups and target organizations. After mapping the Phrase to an entity, the normal *entity to metrics* and *entity to RF document* transforms are available.

MALTEGO MACHINES

These Transforms were designed to be very specific and self-explanatory. However, this approach often means that completing a task involves progressively running many Transforms.

Machines are macro scripts that automate this task to save you time. The integration includes a *Doc Expand* machine for each Entity.



The screenshot shows a window titled "Machine Manager" with a search bar and a list of machines. Each machine has a checkbox, a gear icon, a name, a status, an author, a description, and a read-only checkbox.

	Name	Status	Author	Description	Read-only
<input checked="" type="checkbox"/>	rfASDocExpand	Enabled	Recorded Fut...	Retrieves and expands RF Docs involving an AS Number	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	rfDomainDocExpand	Enabled	Recorded Fut...	Retrieves and expands RF Docs involving a Domain	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	rfEmailDocExpand	Enabled	Recorded Fut...	Retrieves and expands RF Docs involving an Email Address	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	rfFilenameDocExpand	Enabled	Recorded Fut...	Retrieves and expands RF Docs involving a Vulnerability	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	rfHashDocExpand	Enabled	Recorded Fut...	Retrieves and expands RF Docs involving a Hash	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	rfIPDocExpand	Enabled	Recorded Fut...	Retrieves and expands RF Docs involving an IPv4 Address	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	rfMalSigDocExpand	Enabled	Recorded Fut...	Retrieves and expands RF Docs involving a Malware Signature	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	rfMalwareDocExpand	Enabled	Recorded Fut...	Retrieves and expands RF Docs involving a Malware	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	rfPhraseDocExpand	Enabled	Recorded Fut...	Retrieves and expands RF Docs involving a Phrase	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	rfPhraseMap2Alias	Enabled	Matt Kodama	Maps search keyword phrase to Alias in RF	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	rfPhraseMap2Group	Enabled	Matt Kodama	Maps search keyword phrase to Group in RF	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	rfRegKeyDocExpand	Enabled	Recorded Fut...	Retrieves and expands RF Docs involving a Registry Key	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	rfUrlDocExpand	Enabled	Recorded Fut...	Retrieves and expands RF Docs involving a URL	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	rfVulnDocExpand	Enabled	Recorded Fut...	Retrieves and expands RF Docs involving a Vulnerability	<input checked="" type="checkbox"/>

Close

These Machines first retrieves RF Documents matching the current filter properties, and then for each RF Document expands other TI Entities that are also mentioned in that document.

You can use these Machines directly, and can also use them as templates for creating additional Machines that automatically pivot between information in Recorded Future and information in other threat intelligence services.

GETTING SUPPORT

Please contact **support @ recordedfuture.com** with questions or issues using this integration. We're ready to help! We are also eager to hear your ideas for improving and expanding this integration.

APPENDIX A: TRANSFORM LIST

Name	Input	Name	Input Entity
[RF] ASN to Intel Summary	AS	[RF] Email Address to Intel Summary	Email Address
[RF] ASN to RFDoc	AS	[RF] Email Address to RFDoc	Email Address
[RF] Alias to Intel Summary	Alias	[RF] Filename to Metrics	Filename
[RF] Alias to RFDoc	Alias	[RF] Filename to RFDoc	Filename
[RF] Analyst Note to Attack Vector	AnalystNote	[RF] Hash to Analyst Notes	Hash
[RF] Analyst Note to Domain	AnalystNote	[RF] Hash to Domain	Hash
[RF] Analyst Note to Email	AnalystNote	[RF] Hash to Hash	Hash
[RF] Analyst Note to Filename	AnalystNote	[RF] Hash to IP Address	Hash
[RF] Analyst Note to Hash	AnalystNote	[RF] Hash to Intel Summary	Hash
[RF] Analyst Note to IP Address	AnalystNote	[RF] Hash to Malware	Hash
[RF] Analyst Note to Malware	AnalystNote	[RF] Hash to RFDoc	Hash
[RF] Analyst Note to Malware Category	AnalystNote	[RF] Hash to URL	Hash
[RF] Analyst Note to Malware Signature	AnalystNote	[RF] Hash to Vulnerability	Hash
[RF] Analyst Note to Registry Key	AnalystNote	[RF] IP to ASN	IPv4 Address
[RF] Analyst Note to URL	AnalystNote	[RF] IP to Analyst Notes	IPv4 Address
[RF] Analyst Note to	AnalystNote	[RF] IP to Domain	IPv4 Address

Vulnerability			
[RF] Attack Vector to Intel Summary	Attack Vector	[RF] IP to Hash	IPv4 Address
[RF] Attack Vector to RFDoc	Attack Vector	[RF] IP to IP Address	IPv4 Address
[RF] Company to Intel Summary	Company	[RF] IP to Intel Summary	IPv4 Address
[RF] Company to RFDoc	Company	[RF] IP to Location	IPv4 Address
[RF] Domain to Analyst Notes	Domain	[RF] IP to Malware	IPv4 Address
[RF] Domain to Domain	Domain	[RF] IP to Organization	IPv4 Address
[RF] Domain to Hash	Domain	[RF] IP to RFDoc	IPv4 Address
[RF] Domain to IP Address	Domain	[RF] IP to URL	IPv4 Address
[RF] Domain to Intel Summary	Domain	[RF] IP to Vulnerability	IPv4 Address
[RF] Domain to Malware	Domain	[RF] MX Record to Analyst Notes	MX Record
[RF] Domain to RFDoc	Domain	[RF] MX Record to Domain	MX Record
[RF] Domain to URL	Domain	[RF] MX Record to Hash	MX Record
[RF] Domain to Vulnerability	Domain	[RF] MX Record to IP	MX Record
[RF] MX Record to Intel Summary	MX Record	[RF] Operation to Metrics	Operation
[RF] MX Record to Malware	MX Record	[RF] Operation to RFDoc	Operation
[RF] MX Record to RFDoc	MX Record	[RF] Organization to Intel Summary	Organization
[RF] MX Record to URL	MX Record	[RF] Organization to RFDoc	Organization

[RF] MX Record to Vulnerability	MX Record	[RF] Phrase to Alias	Phrase
[RF] Malware Category to RFDoc	Malware Category	[RF] Phrase to Company	Phrase
[RF] Malware Sig to Metrics	Malware Signature	[RF] Phrase to Intel Summary	Phrase
[RF] Malware Sig to RFDoc	Malware Signature	[RF] Phrase to Operation	Phrase
[RF] Malware to Analyst Notes	Malware	[RF] Phrase to Organization	Phrase
[RF] Malware to Domain	Malware	[RF] Phrase to RFDoc	Phrase
[RF] Malware to Email	Malware	[RF] Phrase to RFSource	Phrase
[RF] Malware to Hash	Malware	[RF] RFDoc to Attack Vector	Recorded Future Doc
[RF] Malware to IP	Malware	[RF] RFDoc to Domain	Recorded Future Doc
[RF] Malware to Intel Summary	Malware	[RF] RFDoc to Filename	Recorded Future Doc
[RF] Malware to Malware	Malware	[RF] RFDoc to Hash	Recorded Future Doc
[RF] Malware to RFDoc	Malware	[RF] RFDoc to IP Address	Recorded Future Doc
[RF] Malware to URL	Malware	[RF] RFDoc to Malware	Recorded Future Doc
[RF] Malware to Vulnerability	Malware	[RF] RFDoc to Malware Category	Recorded Future Doc
[RF] Mutex to RFDoc	Mutex	[RF] RFDoc to Malware Signature	Recorded Future Doc
[RF] NS Record to Analyst Notes	NS Record	[RF] RFDoc to RFSource	Recorded Future Doc

[RF] NS Record to Domain	NS Record	[RF] RFDoc to Registry Key	Recorded Future Doc
[RF] NS Record to Hash	NS Record	[RF] RFDoc to URL	Recorded Future Doc
[RF] NS Record to IP	NS Record	[RF] RFDoc to Vulnerability	Recorded Future Doc
[RF] NS Record to Intel Summary	NS Record	[RF] Registry Key to Intel Summary	Registry Entry
[RF] NS Record to Malware	NS Record	[RF] Registry Key to RFDoc	Registry Entry
[RF] NS Record to RFDoc	NS Record	[RF] URL to Intel Summary	URL
[RF] NS Record to URL	NS Record	[RF] URL to RFDoc	URL
[RF] NS Record to Vulnerability	NS Record	[RF] Vulnerability to Analyst Notes	Vulnerability
[RF] Vulnerability to Domain	Vulnerability	[RF] Vulnerability to URL	Vulnerability
[RF] Vulnerability to Hash	Vulnerability	[RF] Vulnerability to Vulnerability	Vulnerability
[RF] Vulnerability to IP	Vulnerability	[RF] Vulnerability to RFDoc	Vulnerability
[RF] Vulnerability to Intel Summary	Vulnerability	[RF] Vulnerability to Malware	Vulnerability