EclecticIQ

Intelligence at the core

Intelligence Hunting Response

How to Create Effective Structured Intelligence Extensions for TIPs

Peter Ferguson

CTI Specialist, EclecticIQ

Who am I

- Cyber Threat Intelligence Specialist, EclecticIQ
- Previously responsible for designing extensions for the EclecticIQ Intelligence Centre
- Now doing threat research for EclecticIQ's Intelligence & Research group

Aim of the Talk

- Convey lessons learned from designing extensions for a threat intelligence platform
- Define requirements needed to start building structured intelligence extensions
- Detail the key goals of an extension
- Help analysts / engineers create extensions that work for them

Key Concepts

What is a TIP?

A centralised platform to ingest, normalise, correlate and analyze threat data from various sources to help support defensive operations

What is Structured Threat Data?

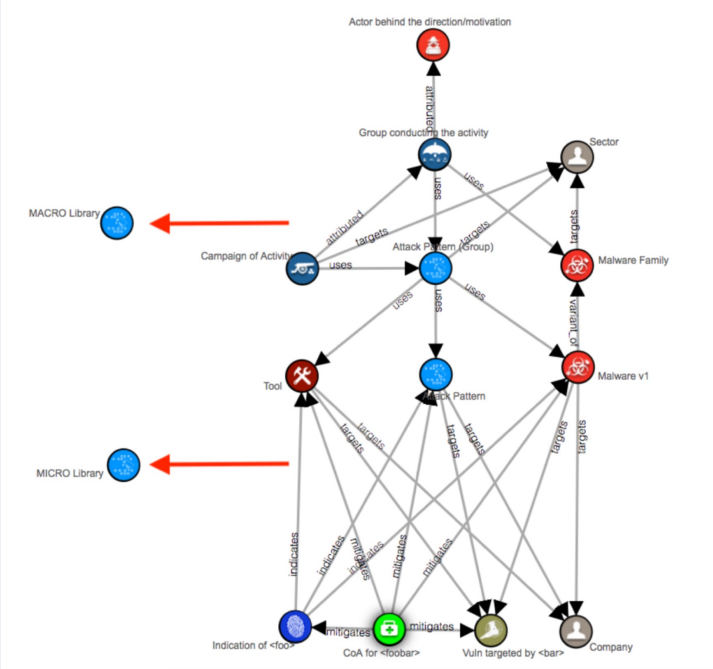
Structured Threat Data is information about cyber security threats that is consistent and machine readable. This is to improve system-to-system sharing, threat analysis and automation.

What are Extensions?

An extension is an add on to the TIP that allows for the ingestion of data from an external source or platform into the TIP; e.g. an incoming feed or an enricher.

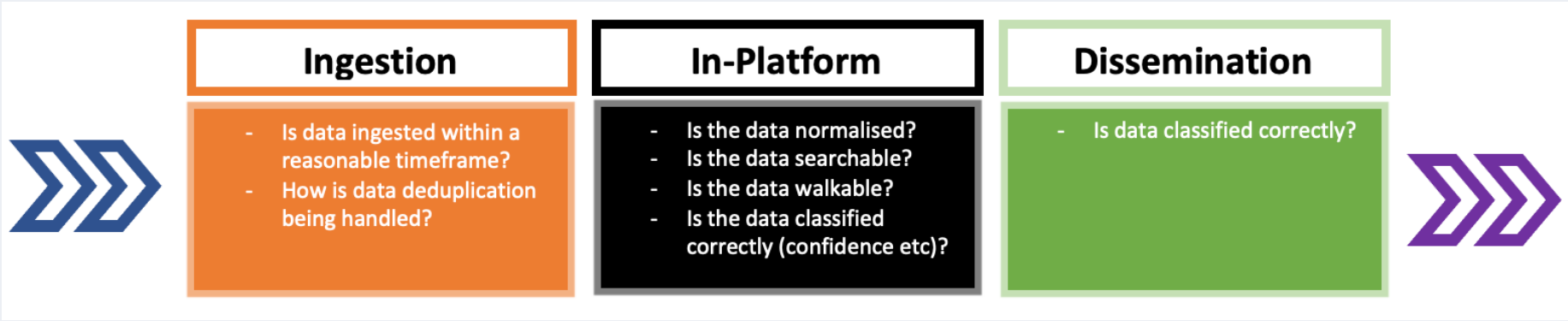
Extensions exist to transform incoming data into a single consistent model and to provide flexibility for the TIP.

Define Your Data Model



- How do you want to represent threat data?
- What are the limitations of the platform you use?
- Can get inspirations from open source standards (STIX)

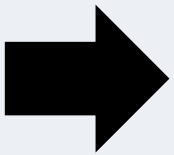
The Data Life Cycle

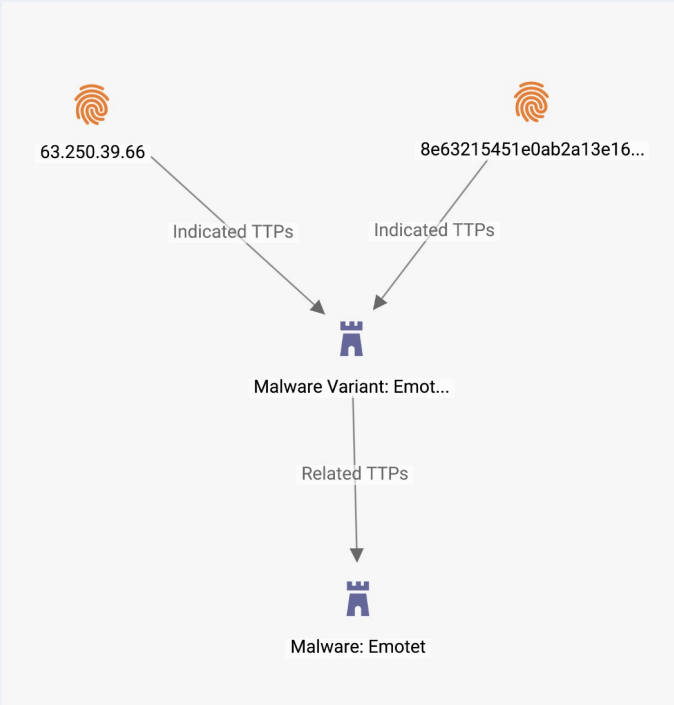


Ingestion

Source Data Including IDs


```
{
    "malware_data": [{
        "sample_1": [{
                "id": "1234abcd",
                "type": "ioc",
                "ip": "63.250.39.66",
                "malware": "emotet",
                "tags": ["malware", "windows", "malicious", "downloader", "c2"],
                "timestamp": 1663692836,
                "source": "https://www.eclecticiq.com/"
            },
            {
                "id": "5678ertq",
                "type": "ioc",
                "hash": "8e63215451e0ab2a13e16494a2fab97bb507f36684738268f564fa2238160c38",
                "malware": "emotet",
                "tags": ["malware", "windows", "malicious", "downloader"],
                "timestamp": 1663692836,
                "source": "https://www.eclecticiq.com/"
            },
            {
                "id": "1234abcd",
                "type": "ioc",
                "ip": "63.250.39.66",
                "malware": "emotet",
                "tags": ["malware", "windows", "malicious", "downloader", "c2"],
                "timestamp": 1663692836,
                "source": "https://www.eclecticiq.com/"
            }
        ]
    }]
}
```

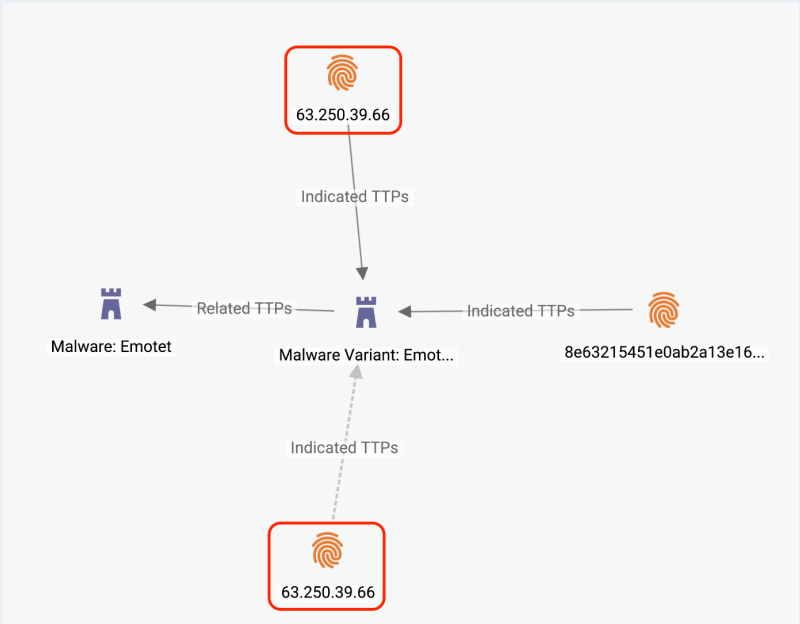





EclecticIQ Intelligence at the core

Source Data Without IDs

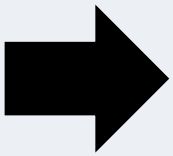

```
{
    "malware_data": [{
        "sample_1": [{
                "type": "ioc",
                "ip": "63.250.39.66",
                "malware": "emotet",
                "tags": ["malware", "windows", "malicious", "downloader", "c2"],
                "timestamp": 1663692836,
                "source": "https://www.eclecticiq.com/"
            },
            {
                "type": "ioc",
                "hash": "8e63215451e0ab2a13e16494a2fab97bb507f36684738268f564fa2238160c38",
                "malware": "emotet",
                "tags": ["malware", "windows", "malicious", "downloader"],
                "timestamp": 1663692836,
                "source": "https://www.eclecticiq.com/"
            },
            {
                "type": "ioc",
                "ip": "63.250.39.66",
                "malware": "emotet",
                "tags": ["malware", "windows", "malicious", "downloader", "c2"],
                "timestamp": 1663692836,
                "source": "https://www.eclecticiq.com/"
            }
        ]
    }]
}
```

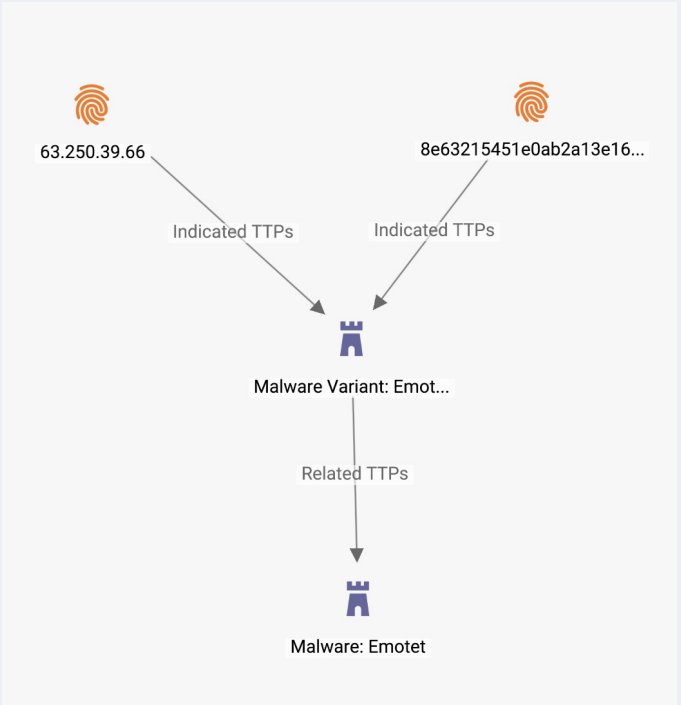



EclecticIQ Intelligence at the core

How to Fix - Source Data Without IDs


```
{
    "malware_data": [{
        "sample_1": [{
                "type": "ioc",
                "ip": "63.250.39.66",
                "malware": "emotet",
                "tags": ["malware", "windows", "malicious", "downloader", "c2"],
                "timestamp": 1663692836,
                "source": "https://www.eclecticiq.com/"
            },
            {
                "type": "ioc",
                "hash": "8e63215451e0ab2a13e16494a2fab97bb507f36684738268f564fa2238160c38",
                "malware": "emotet",
                "tags": ["malware", "windows", "malicious", "downloader"],
                "timestamp": 1663692836,
                "source": "https://www.eclecticiq.com/"
            },
            {
                "type": "ioc",
                "ip": "63.250.39.66",
                "malware": "emotet",
                "tags": ["malware", "windows", "malicious", "downloader", "c2"],
                "timestamp": 1663692836,
                "source": "https://www.eclecticiq.com/"
            }
        ]
    }]
}
```

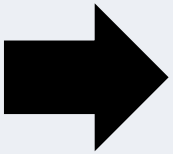


EclecticIQ Intelligence at the core

Targeted Collection


```
{
    "search_result_data": [{
        "type": "ioc",
        "hash": "b2f58eda1180aa69c80d68d070b29f62c21ebd9cdc18266a46fbd991e3f36a88",
        "malware": "emotet_document",
        "tags": ["malware", "windows", "malicious", "downloader"],
        "timestamp": 1663692836,
        "source": "https://www.eclecticiq.com/",
        "search": "behaviour_network:https://213.239.212.5:443/"
    }]
}

{
    "search_result_data": [{
        "type": "ioc",
        "hash": "b2f58eda1180aa69c80d68d070b29f62c21ebd9cdc18266a46fbd991e3f36a88",
        "malware": "emotet_document",
        "tags": ["malware", "windows", "malicious", "downloader"],
        "timestamp": 1663692836,
        "source": "https://www.eclecticiq.com/",
        "search": "content:{6F 6E 22 2C 22 55 52 4C 44 6F 77 6E 6C 6F 61 64 54 6F 46 69 6C}"
    }]
}
```

b2f58eda1180aa69c80d6...

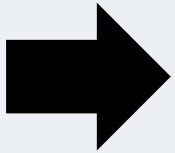
b2f58eda1180aa69c80d6...

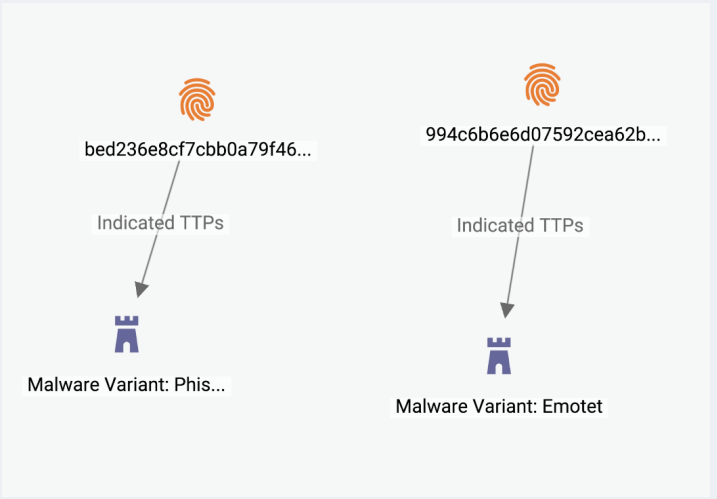
EclecticIQ Intelligence at the core

In-Platform

Making Assumptions on Data


```
{
    "data": [{
        "type": "ioc",
        "hash": "994c6b6e6d07592cea62bd2b667c60694e862f17f7e74088feb8d964595f10ba",
        "threat": "emotet",
        "tags": ["malware", "windows", "malicious", "downloader"],
        "timestamp": 1663692836,
        "source": "https://www.eclecticiq.com/",
    },
    {
        "type": "ioc",
        "hash": "bed236e8cf7cbb0a79f4620fdbfb84796269a3eb8ec332b7b664375e1ed9627a",
        "threat": "phishing",
        "tags": ["phishing", "malicious"],
        "timestamp": 1663701184,
        "source": "https://www.eclecticiq.com/",
    }]
}
```

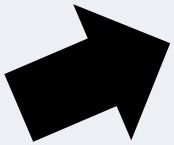



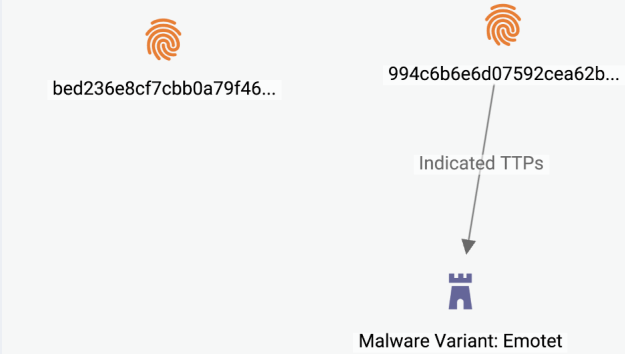


How to Fix - Making Assumptions on Data


```
{
    "data": [{
        "type": "ioc",
        "hash": "994c6b6e6d07592cea62bd2b667c60694e862f17f7e74088feb8d964595f10ba",
        "threat": "emotet",
        "tags": ["malware", "windows", "malicious", "downloader"],
        "timestamp": 1663692836,
        "source": "https://www.eclecticiq.com/",
    },
    {
        "type": "ioc",
        "hash": "bed236e8cf7cbb0a79f4620fdbfb84796269a3eb8ec332b7b664375e1ed9627a",
        "threat": "phishing",
        "tags": ["phishing", "malicious"],
        "timestamp": 1663701184,
        "source": "https://www.eclecticiq.com/",
    }]
}
```


1. Create Logic



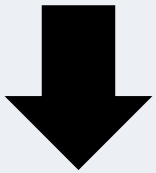


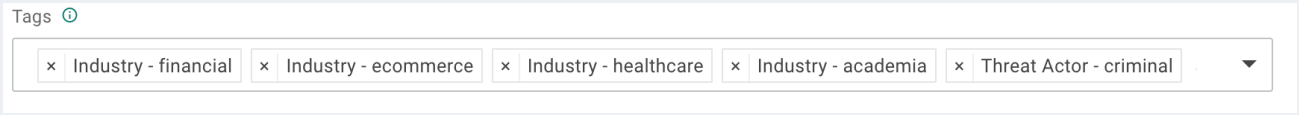
2. Flatten

EclecticIQ Intelligence at the core

Leverage Platform Automation Capabilities


```
{
    "data": [{
        "type": "ioc",
        "hash": "994c6b6e6d07592cea62bd2b667c60694e862f17f7e74088feb8d964595f10ba",
        "malware": "emotet",
        "tags": ["malware", "windows", "malicious", "downloader"],
        "industries": ["financial", "ecommerce", "healthcare", "Academia"],
        "actor_type": ["criminal"]
        "timestamp": 1663692836,
        "source": "https://www.eclecticiq.com/",
    }]
}
```

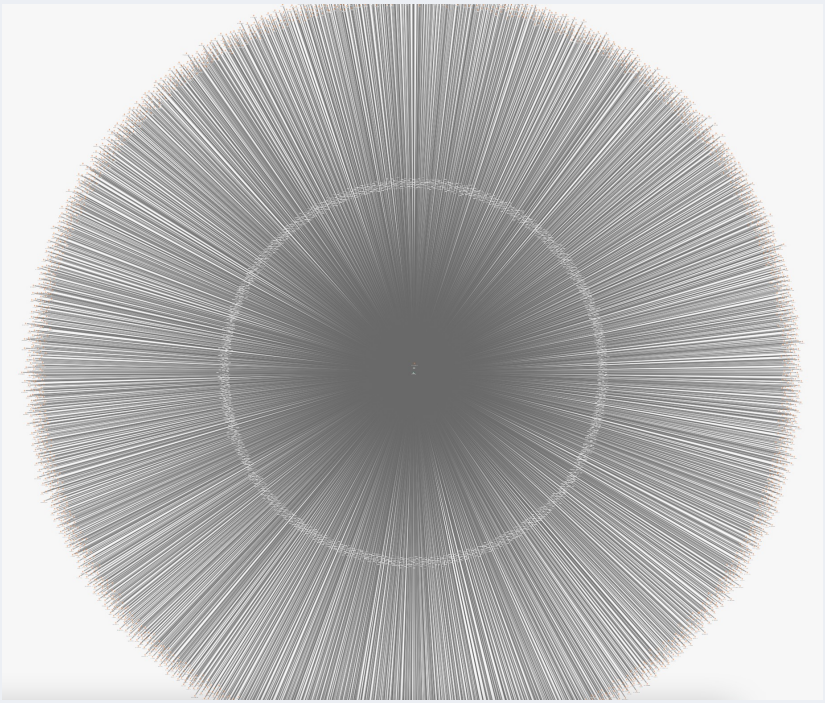





EclecticIQ Intelligence at the core

Too Much Related Data

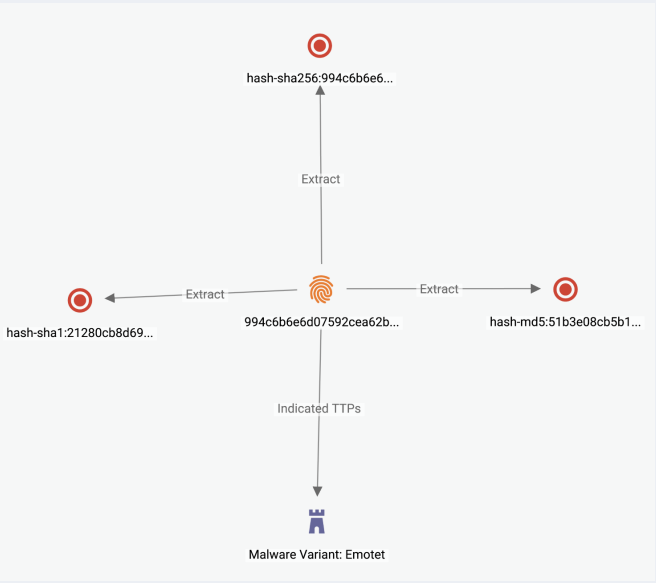

```
{
    "data": [{
        "type": "ioc",
        "sha256_hash": "994c6b6e6d07592cea62bd2b667c60694e862f17f7e74088feb8d964595f10ba",
        "sha1_hash": "21280cb8d696d79f68e9bb99661d77aaddfa97c1",
        "md5_hash": "51b3e08cb5b18fd46876b4a9bebb0fd0",
        "malware": "emotet",
        "tags": ["malware", "windows", "malicious", "downloader"],
        "industries": ["financial", "ecommerce", "healthcare", "Academia"],
        "actor_type": ["criminal"]
        "timestamp": 1663692836,
        "source": "https://www.eclecticiq.com/",
        "observables": [
            "d8531a1ac331414d357ac014ac8813b93c2c0ea1756542ad8bacb6d352ed4891",
            "bf96645a2721720fbe8fc0a47a243d73d5901e6213eb01c6eca976ab9bc18235",
```

EclecticIQ Intelligence at the core

How to Fix - Too Much Related Data


```
{
    "data": [{
        "type": "ioc",
        "sha256_hash": "994c6b6e6d07592cea62bd2b667c60694e862f17f7e74088feb8d964595f10ba",
        "sha1_hash": "21280cb8d696d79f68e9bb99661d77aaddfa97c1",
        "md5_hash": "51b3e08cb5b18fd46876b4a9bebb0fd0",
        "malware": "emotet",
        "tags": ["malware", "windows", "malicious", "downloader"],
        "industries": ["financial", "ecommerce", "healthcare", "Academia"],
        "actor_type": ["criminal"]
        "timestamp": 1663692836,
        "source": "https://www.eclecticiq.com/",
        "observables": [
            "d8531a1ac331414d357ac014ac8813b93c2c0ea1756542ad8bacb6d352ed4891",
            "bf96645a2721720fbe8fc0a47a243d73d5901e6213eb01c6eca976ab9bc18235",
            "89e5b747ac600f96b062052582002ac25d083f5a461d26af0fb184f57b7754fd",
        ]
    }]
}
```

EclecticIQ Intelligence at the core

Consistent Classification

```
{
    "data": [{
        "type": "ioc",
        "sha256_hash": "994c6b6e6d07592cea62bd2b667c60694e862f17f7e74088feb8d964595f10ba",
        "sha1_hash": "21280cb8d696d79f68e9bb99661d77aaddfa97c1",
        "md5_hash": "51b3e08cb5b18fd46876b4a9bebb0fd0",
        "confidence": "50"
        "malware": "emotet",
        "tags": ["malware", "windows", "malicious", "downloader"],
        "industries": ["financial", "ecommerce", "healthcare", "Academia"],
        "actor_type": ["criminal"]
        "timestamp": 1663692836,
        "source": "https://www.eclecticiq.com/",
    }]
}
```

Classification	Number
Unknown	N/A
None	0
Low	1-33
Medium	34-66
High	67-100

EclecticIQ Intelligence at the core

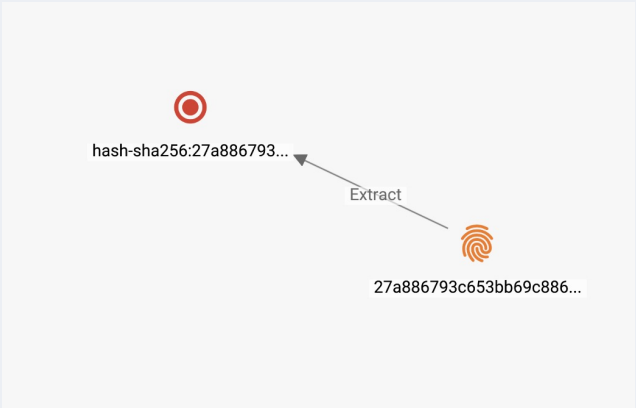
Dissemination

Extension Tips for Dissemination

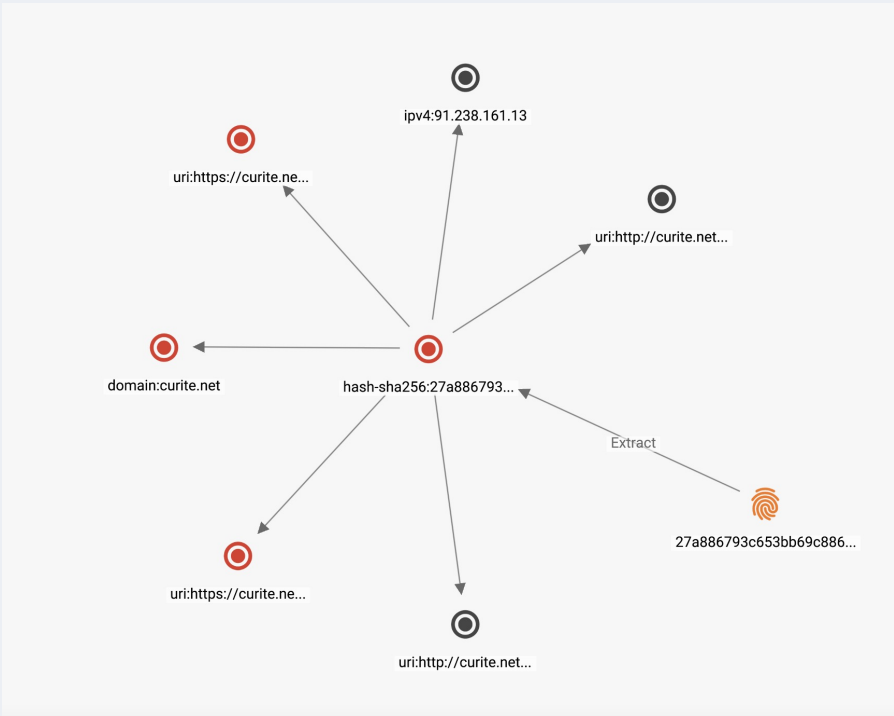
- The bulk of dissemination is automated
- Exact process will be platform dependent
- All platforms will use some kind of filtering
- This stage is reliant on good design decisions in the earlier stages

Enrichers

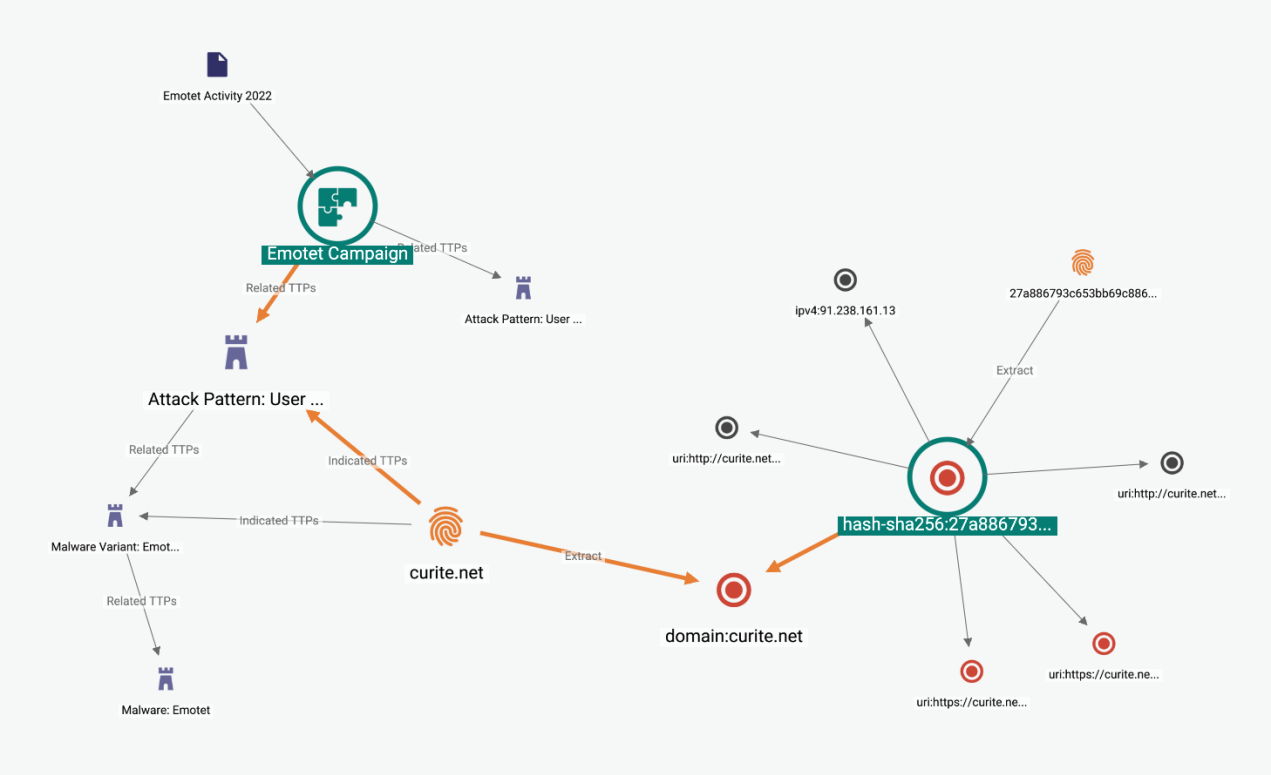
Granular Enrichers



What is the infrastructure used to download this file?



Enricher in Use



EclecticIQ Intelligence at the core

Key Goals & Tips

Goals & Tips

Key Goals

- Ingestion of data within a reasonable timeframe
- Normalisation of data into a single model
- Correct classification of data
- Enrichment is granular

Tips to takeaway

- Keep it simple
- If the platform can do it, let it
- Avoid assumptions on data
- The extension is only as strong as its weakest link
- Extensions are about making the correct trade-offs between all stakeholders

EclecticIQ

Intelligence at the core

Intelligence Hunting Response

Any Questions?

blog.eclecticiq.com