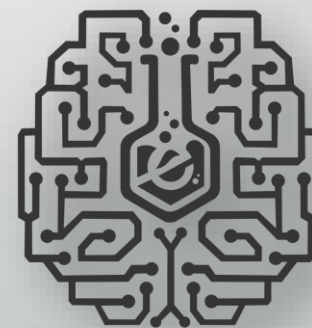




Cratos

Use your **bloody** indicators



eCrimeLabs

<https://www.ecrimelabs.com>



About @DennisRand

Founder of eCrimeLabs

Providing Managed and hosted MISP services, and also working with incident response and threat intelligence.

Been a heavy user of MISP since around 2015



<https://www.ecrimelabs.com>



@DennisRand
@eCrimelabs

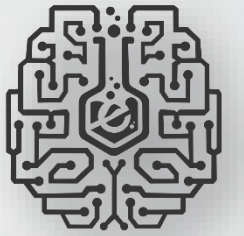


Spare time kayaking and a bit of swimming

A Case

A Problem

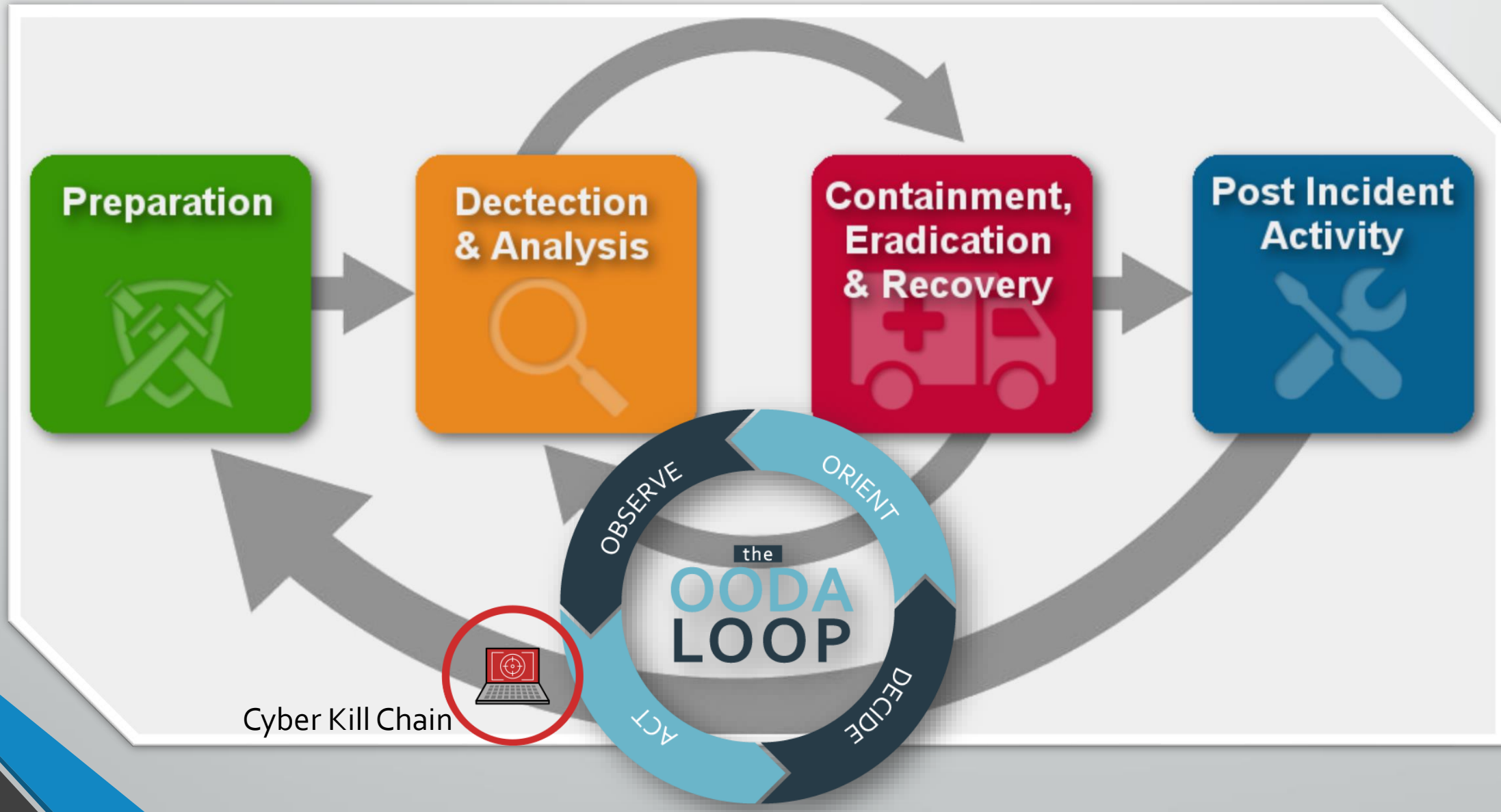
A Solution



eCrimeLabs



Incident Life-cycle



The Case – Initial alert

Source: <https://thefirreport.com/2023/06/12/a-truly-graceful-wipe-out/>



So lets say your first alert is here

16:19 UTC TrueBot loads Cobalt Strike

C:\Intel\RuntimeBroker.exe creates cmd.exe and accesses process

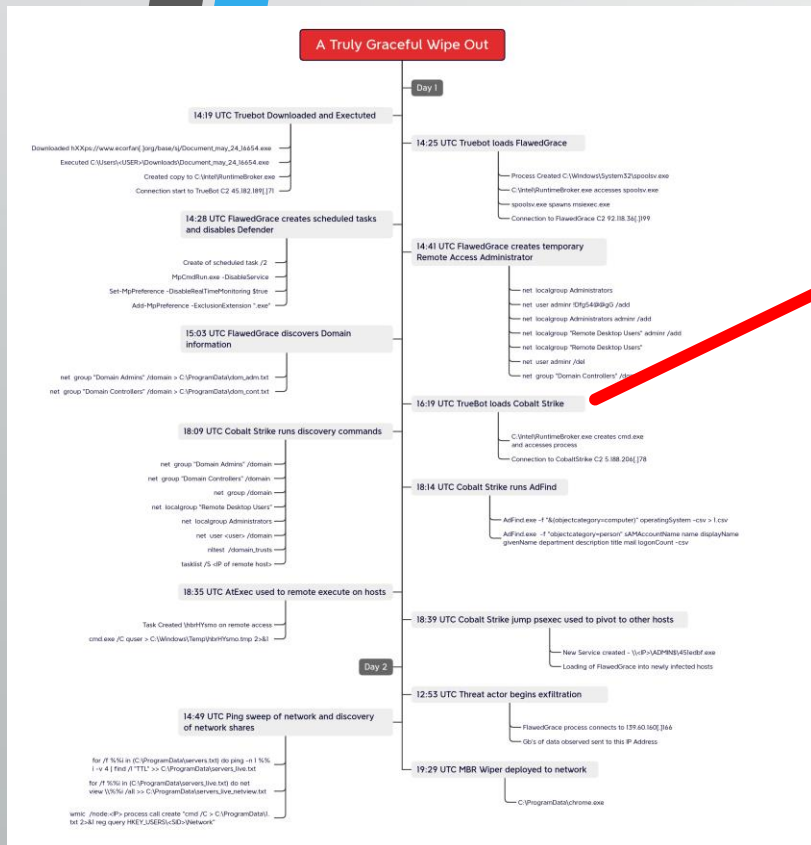
Connection to CobaltStrike C2 5.188.206[.178]



Anti virus

The triage starts utilizing all sources available

SIEM



The Case – Initial Triage

Source: <https://thedfirreport.com/2023/06/12/a-truly-graceful-wipe-out/>



MD5: 6164e9d297d29aa8682971259da06848 → Truebot

SHA1: 96b95edc1a917912a3181d5105fd5bfad1344de0 → Truebot

SHA256: 717beedcd2431785a0f59d194e47970e9544fbf398d462a305f6ad9a1b1100cb → Truebot



hxxps://5.188.206.78 → Cobalt Strike

hxxps://essadonio.com → Truebot



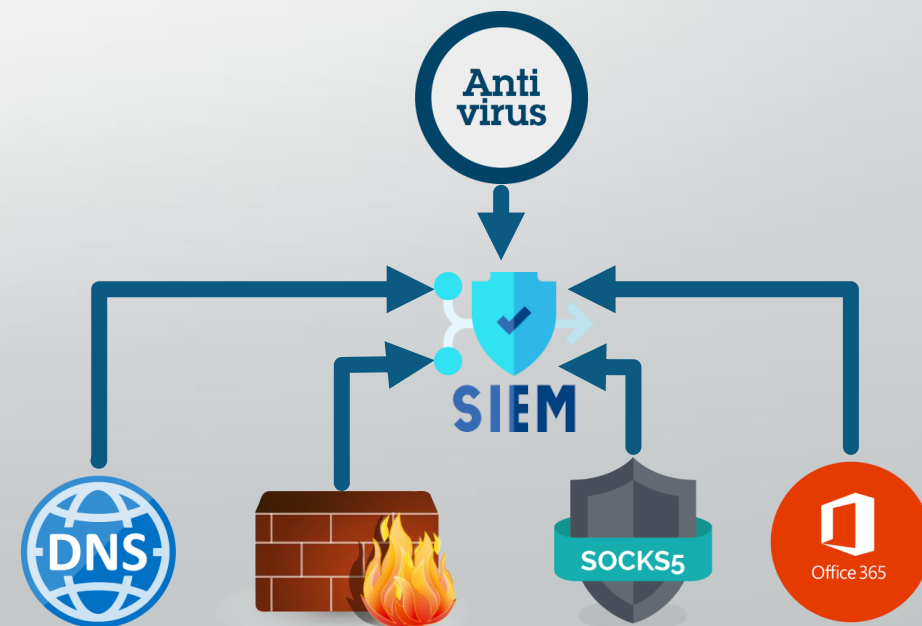
essadonio.com → Truebot

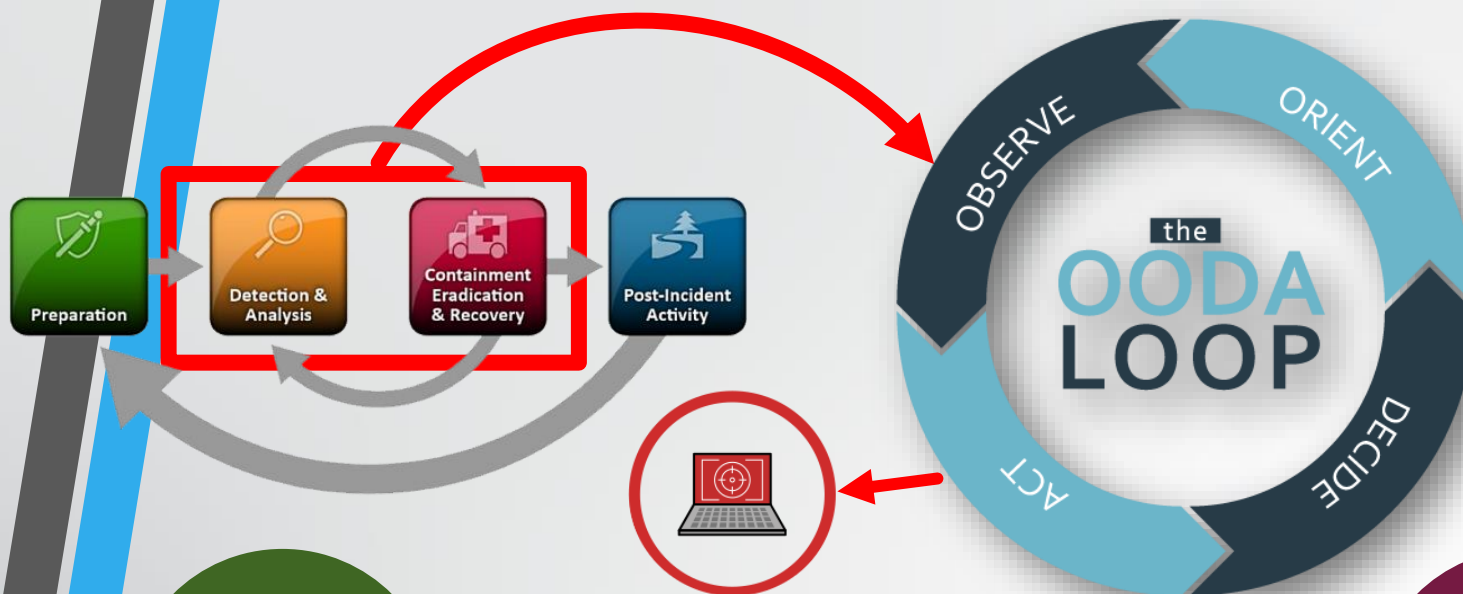


5.188.206.78 → Cobalt Strike

45.182.189.71 → Truebot

5.188.86.18 → FlawedGrace





Course of Action Cyber Kill Chain

Passive

Active

Discover

Detect

Deny

Disrupt

Degrade

Deceive

Destroy

MAKE GOOD CHOICES





People is part of the problem

Active - Blocking



Would **you** be able to make **changes** across multiple systems and technologies **within 10-15 minutes** when you need it ?

AND what if you make a mistake and want it removed again ?



6164e9d297d29aa8682971259da06848



hxxps://5.188.206.78/
hxxps://essadonio.com



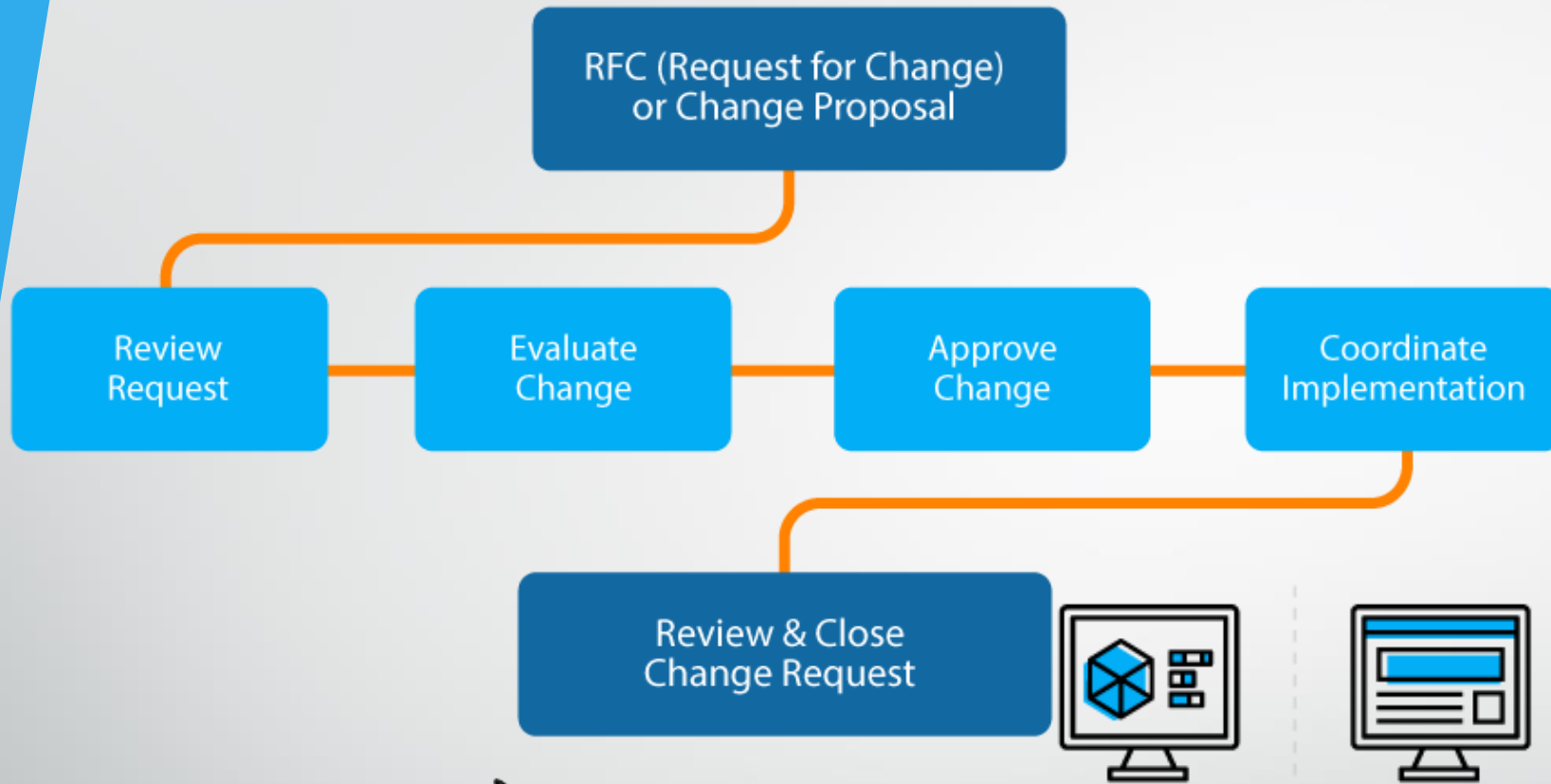
essadonio.com



5.188.206.78
45.182.189.71
5.188.86.18
8.8.8.8



Processes, Technology and People



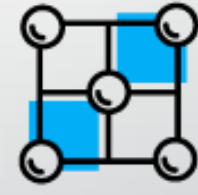
STANDARD

- Straightforward
- Frequent
- Documentation needed
- No authorization by CAB needed



NORMAL

- Important
- Full review
- Requires CAB authorization



MAJOR

- High risk
- Detailed report
- Requires CAB & management authorization



EMERGENCY

- Urgent
- Resolves incident
- High risk of failure
- Flexible pool of approvers

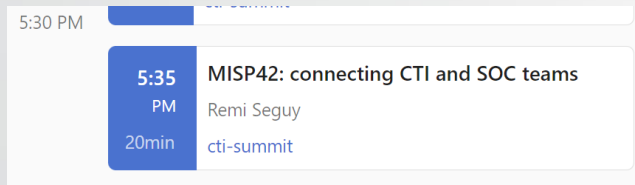
MISP to the rescue

Challenges and a solution



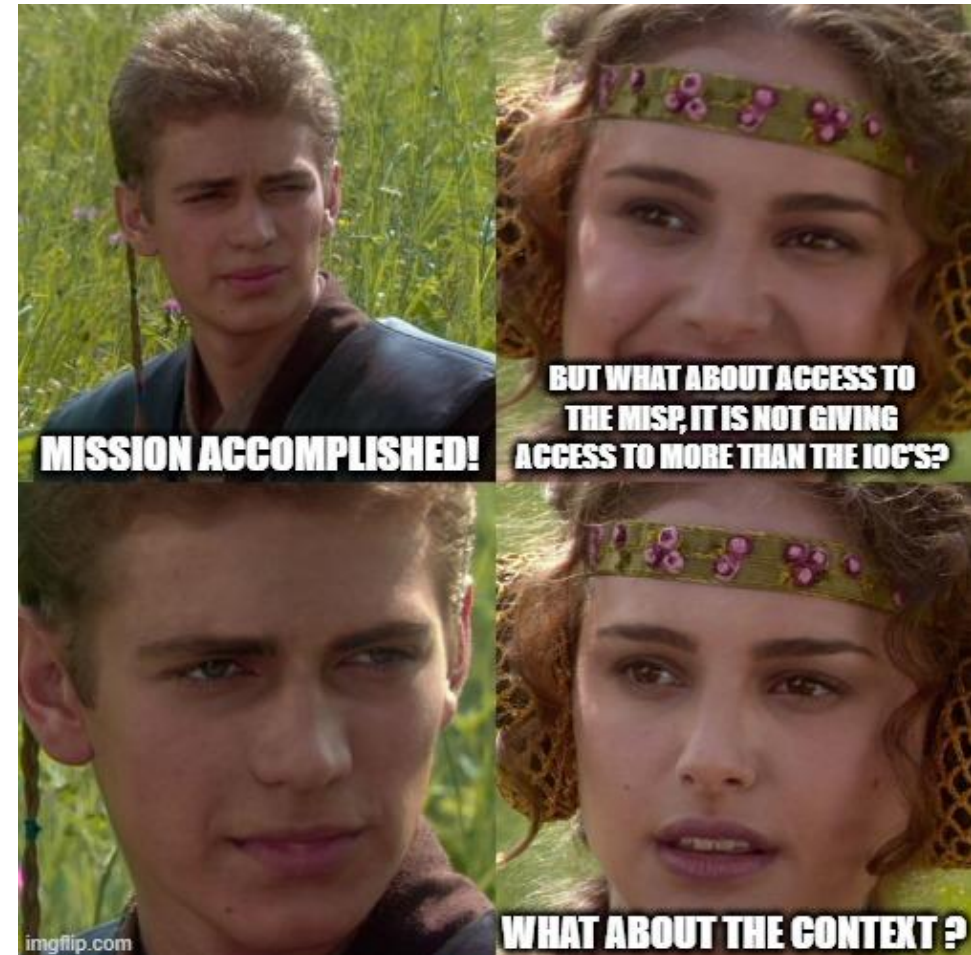
Just integrate MISP data into your security components

There are exists many good integrations to MISP today - Later today



But some of the key challenges

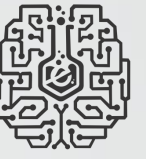
- API tokens gives access to **read all data**, however, can be IP restricted.
- Having multiple systems query the MISP instance constantly can result in a **bottle neck** of resources.
- In some cases your ingestion systems only support IPv4 but what about data in CIDR
- What if your MISP instance is **only** available from internal IP's





CRATOS





Short history lesson of the name

In Greek mythology, **Kratos**, also known as **Cratus** or **Cratos**.

Cratos was, for the Ancient Greeks, a personification of brute strength or power.

What is Cratos

Cratos is utilizing the **FastAPI framework** to build a REST API, written in **Python** with a **Memcached** in the backend allowing for:

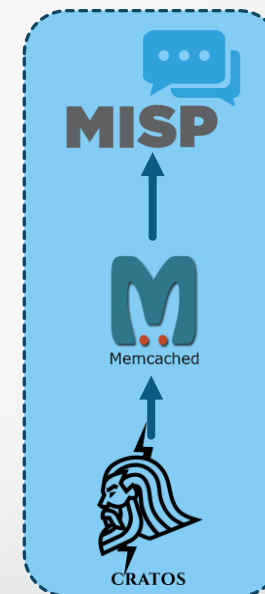
- **Easy integration** into security products and making MISP data available to analysts, **without giving full access to the MISP instance** and thereby protecting the context around indicators.
- It has the support for acting as a **caching proxy** allowing multiple systems to get the same data rapidly without putting unnecessary pressure on the MISP instances.
- Also support **one entry to multiple MISP instances**.
- Keeping the **query in the URI** allows more systems to be able to fetch the data, without additional code, **but** also support it as a token.
- De-duplication and sanity check(Regex) of indicators.

Infrastructure

Keeping it **simple** or making it **complex**

Simple

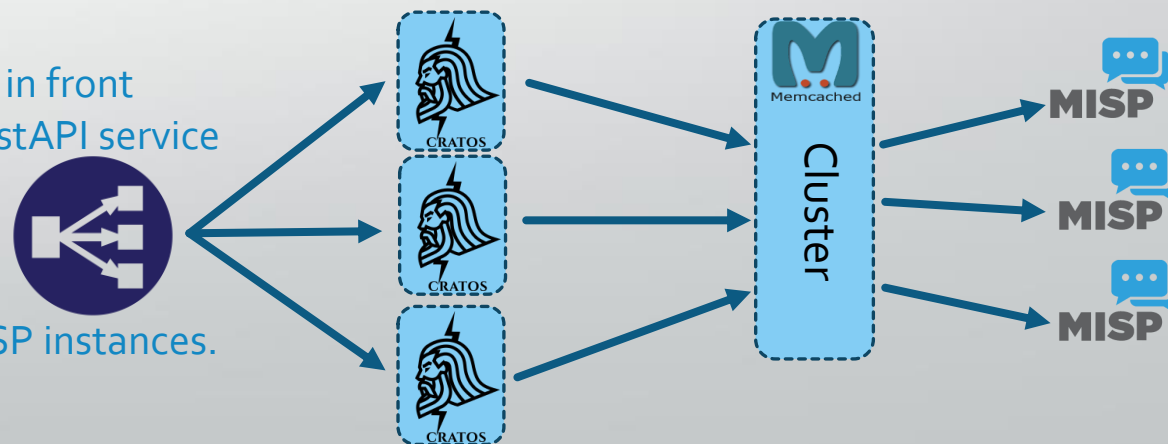
One API to one MISP instance on same server



More Complex

You can add a load balancer in front and have as many Cratos FastAPI service running.

Communicating with a Memcached cluster and querying to one or more MISP instances.





eCrimeLabs

Structure and security model

For each MISP instance that Cratos has to connect to there is a config file

- Whitelisted IP ranges
- Besides the expiration on the MISP API key, you add an expiration key for this specific
- A pre-tagging is created for mapping
- Encryption of the auth key is currently utilizing "PBKDF2-HMAC-SHA-256" with 600.000 iterations

```
{
  "enabled": true,
  "debug": false,
  "company": "eCrimeLabs ApS",
  "tag": "ecrimelabs",
  "mispVerifyCert": true,
  "mispTimeoutSeconds": 100,
  "mispDebug": true,
  "memcached_all_timeout": 300,
  "falsepositive_timeout": "1w",
  "list_stats": "1w",
  "allowed_ips": [
    "10.0.0.0/8",
    "127.0.0.1/32",
    "192.168.1.0/24",
    "172.31.217.0/24",
    "172.31.208.0/24",
    "100.64.3.0/24"
  ],
  "custom_feeds": {
    "cust1": ":incident-classification=cust1",
    "cust2": ":incident-classification=cust2",
    "cust3": ":incident-classification=cust3",
    "cust4": ":incident-classification=cust4",
    "cust5": ":incident-classification=cust5"
  }
}
```

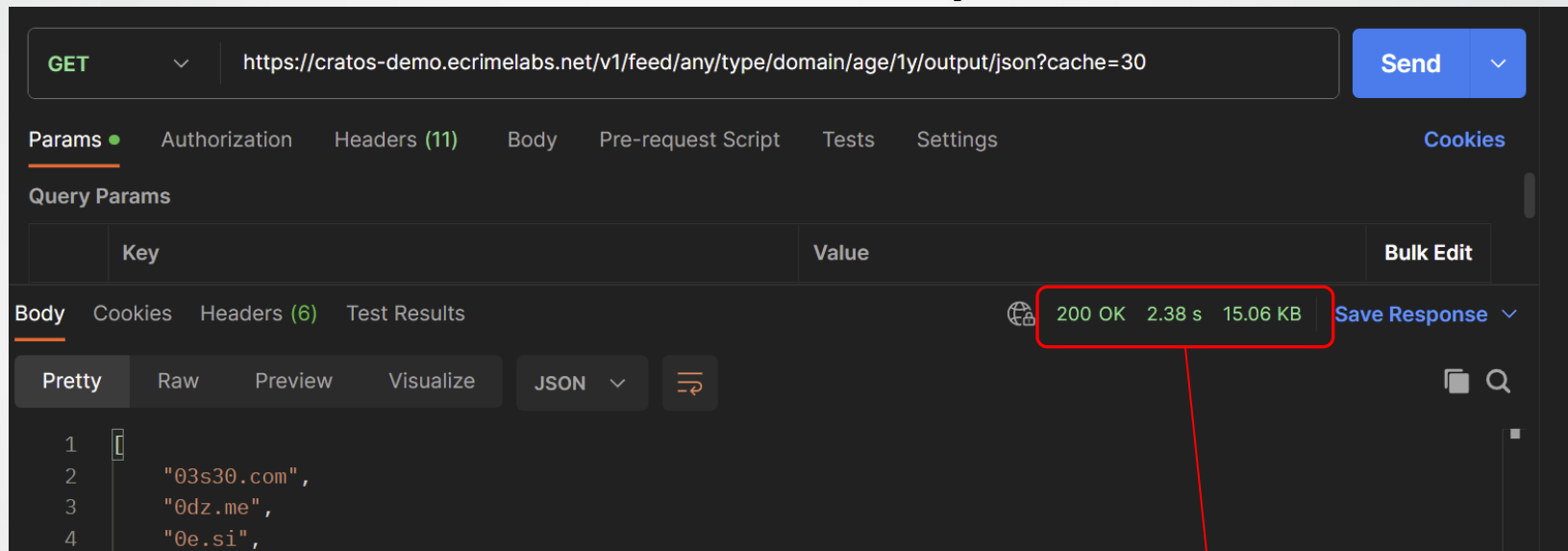
Generate a configuration token for authentication through API

Name	<input type="text" value="https://"/>
FQDN	<input type="text" value="private.ecrimelabs.net"/>
port	<input type="text" value="443"/>
MISP Authentication Key	<input type="text" value="lorem ipsum"/>
Key Expiration	<input type="text" value="22/10/2023"/>

Submit

CRATOS

Caching responses to minimize load on MISP and increase speed



GET `https://cratos-demo.ecrimelabs.net/v1/feed/any/type/domain/age/1y/output/json?cache=30` Send

Params • Authorization Headers (11) Body Pre-request Script Tests Settings Cookies

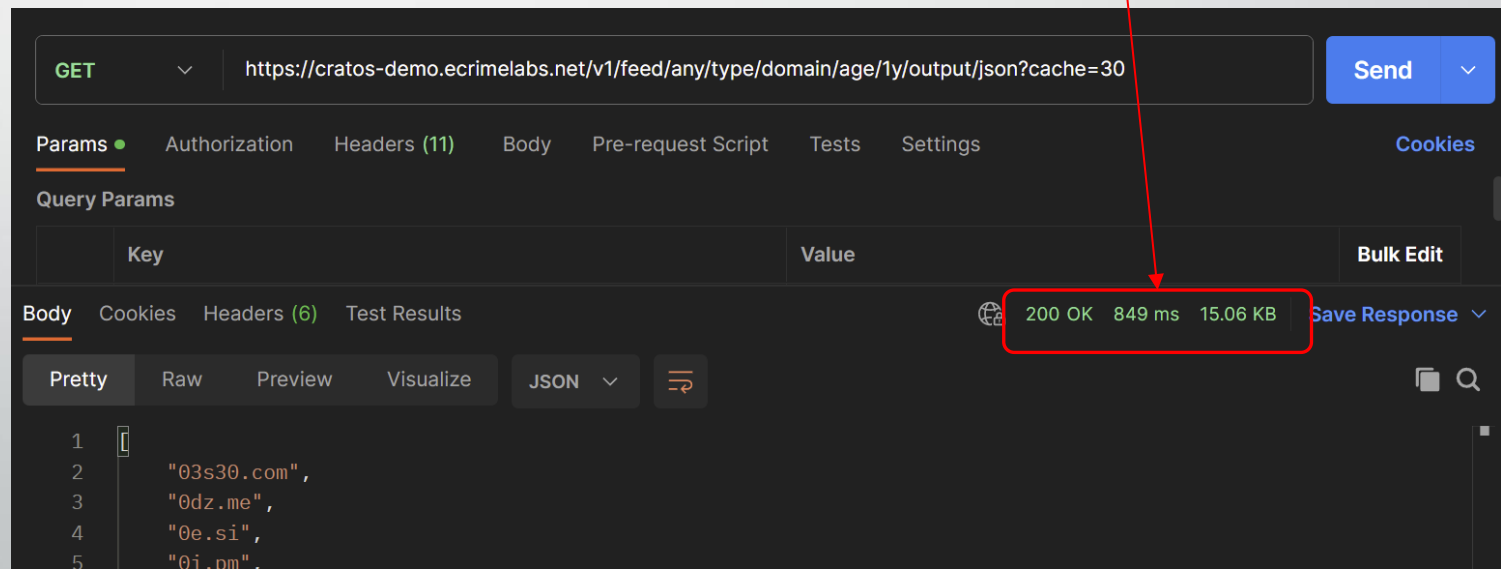
Query Params

Key	Value	Bulk Edit
-----	-------	-----------

Body Cookies Headers (6) Test Results 200 OK 2.38 s 15.06 KB Save Response

Pretty Raw Preview Visualize JSON

```
1 [
2   "03s30.com",
3   "0dz.me",
4   "0e.si",
```



GET `https://cratos-demo.ecrimelabs.net/v1/feed/any/type/domain/age/1y/output/json?cache=30` Send

Params • Authorization Headers (11) Body Pre-request Script Tests Settings Cookies

Query Params

Key	Value	Bulk Edit
-----	-------	-----------

Body Cookies Headers (6) Test Results 200 OK 849 ms 15.06 KB Save Response

Pretty Raw Preview Visualize JSON

```
1 [
2   "03s30.com",
3   "0dz.me",
4   "0e.si",
5   "0i.pm",
```

Implemented requests

default

GET / Homepage

authentication

GET /v1/generate_token_form UI based access to generate the Auth keys

POST /v1/generate_token_json Form Post Json

documentations

GET /v1/openapi.json Get Open Api Endpoint

GET /v1/help Get Documentation

status

GET /v1/check Check connection to MISP

info

GET /v1/statistics Get attribute type statistics from the MISP

GET /v1/warninglist/id/{warninglistId}/output/{returnedDataType} Get lists and content of Warning lists from MISP

DELETE /v1/clear_cache/feed/{feedName}/type/{dataType}/age/{dataAge}/output/{returnedDataType} Delete cached data related to specific feed

feeds

GET /v1/feed/{feedName}/type/{dataType}/age/{dataAge}/output/{returnedDataType} Retrieve data from MISP composed into a simple return format

Choose you feed – MISP Logic

feeds

GET

/v1/feed/{feedName}/type/{dataType}/age/{dataAge}/output/{returnedDataType}

Feed names in Cratos

- incident
- alert
- hunt

- block
- cust1
- cust2
- cust3
- cust4
- cust5

- any

- 42

Mapping and logic in MISP

tags = ecrimelabs:incident-classification=<Feedname>
to_ids = True
enforceWarninglist = True
Published = False

tags = ecrimelabs:incident-classification=<Feedname>
to_ids = True
enforceWarninglist = True
Published = True

tags = *
to_ids = True
enforceWarninglist = True
Published = True

tags = *
to_ids = True
enforceWarninglist = False
Published = True

Name ↓

ecrimelabs:incident-classification=alert

ecrimelabs:incident-classification=block

ecrimelabs:incident-classification=cust1

ecrimelabs:incident-classification=cust2

ecrimelabs:incident-classification=cust3

ecrimelabs:incident-classification=cust4

ecrimelabs:incident-classification=cust5

ecrimelabs:incident-classification=false-positive

ecrimelabs:incident-classification=hunt

ecrimelabs:incident-classification=incident

Mapping the "Type" of MISP data



eCrimeLabs

feeds

GET /v1/feed/{feedName}/type/{dataType}/age/{dataAge}/output/{returnedDataType} |

```
"types": {  
  "ipv4ext": ["ip-src", "ip-dst", "domain|ip", "ip-dst|port", "ip-src|port"],  
  "ipv4": ["ip-src", "ip-dst", "domain|ip", "ip-dst|port", "ip-src|port"],  
  "ipv6": ["ip-src", "ip-dst", "domain|ip", "ip-dst|port", "ip-src|port"],  
  "cidr4": ["ip-src", "ip-dst"],  
  "domain": ["domain"],  
  "hostname": ["hostname", "domain|ip", "hostname|port"],  
  "url": ["url"],  
  "md5": ["md5", "filename|md5"],  
  "sha1": ["sha1", "filename|sha1"],  
  "sha256": ["sha256", "filename|sha256"],  
  "mutex": ["mutex"],  
  "snort": ["snort"],  
  "yara": ["yara"],  
  "sigma": ["sigma"],  
  "x509-fingerprint-md5": ["x509-fingerprint-md5"],  
  "x509-fingerprint-sha1": ["x509-fingerprint-sha1"],  
  "x509-fingerprint-sha256": ["x509-fingerprint-sha256"],  
  "email-address": ["email-dst", "email-src"],  
  "email-subject": ["email-subject"],  
  "email-attachment": ["email-attachment"],  
  "vulnerability": ["vulnerability"],  
  "ja3": ["ja3-fingerprint-md5"],  
  "hassh-md5": ["hassh-md5"],  
  "hasshserver-md5": ["hasshserver-md5"],  
  "imphash": ["imphash"],  
  "crypto-currency": ["btc", "xmr"]  
}
```

CRATOS

Curl

```
curl -X 'GET' \
  'http://cratos.ecrimelabs.org:8080/v1/feed/any/type/domain/age/1m/output/txt?cache=60' \
  -H 'accept: application/json' \
  -H 'token: gAAAAAB1KQ8V9Zivu3y9FJfPU-HEZM3fYQ4c19Z5q3Ly2dws_fesbmjbX81bxAh9uzaNxKEGEX4oA0oGo4-_fjUJnmh_Z22BUTjF9-fNR18U9xpHMIoR80ksBwq-iWz_q77aGzy_8129jj8oQdJmaF0vtsj4aZeZ4rwChSH05zZ9hGRH3wautbLY2WvjLVFKA91'
```

Request URL

http://cratos.ecrimelabs.org:8080/v1/feed/any/type/domain/age/1m/output/txt?cache=60

Server response

Code

Details

200

Response body

benchesmade.us
bestoffernewforu.com
bestwesternnt.com
betly.me
betshopkipstri.com
bik.cityco.top
bikeontop.shop
biqaurall.site
bitshort.info
bitsvertise.com
bitwariden.com
bity.ws
bizmeka.viewdns.net
blgbeach.com
blitzmedia.live
block.descriptionscripts.com
blog.sellygg.tk
blue.theinternetsupply.com
booking.com.id51051062.date
booking.offer282.cloud
bosmata.com
branter.tk
breaknews.live
brkorage.live
bronergerg.tk
bruker-app.com
btlin.life
btscotland.com

Response headers

content-length: 25155
content-type: text/plain; charset=utf-8
date: Fri, 13 Oct 2023 14:28:16 GMT
server: uvicorn
x-cache: HIT

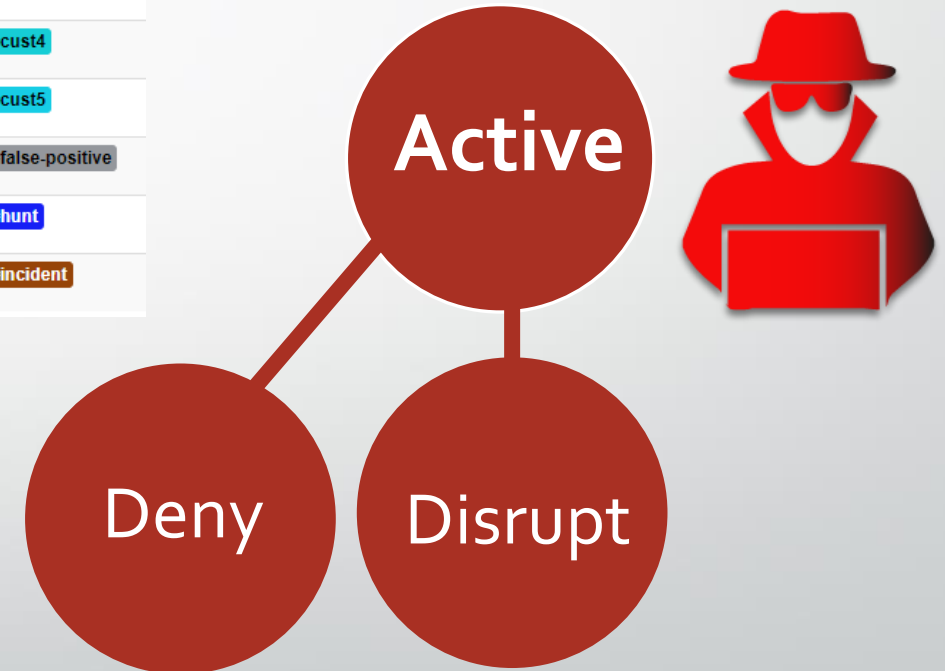
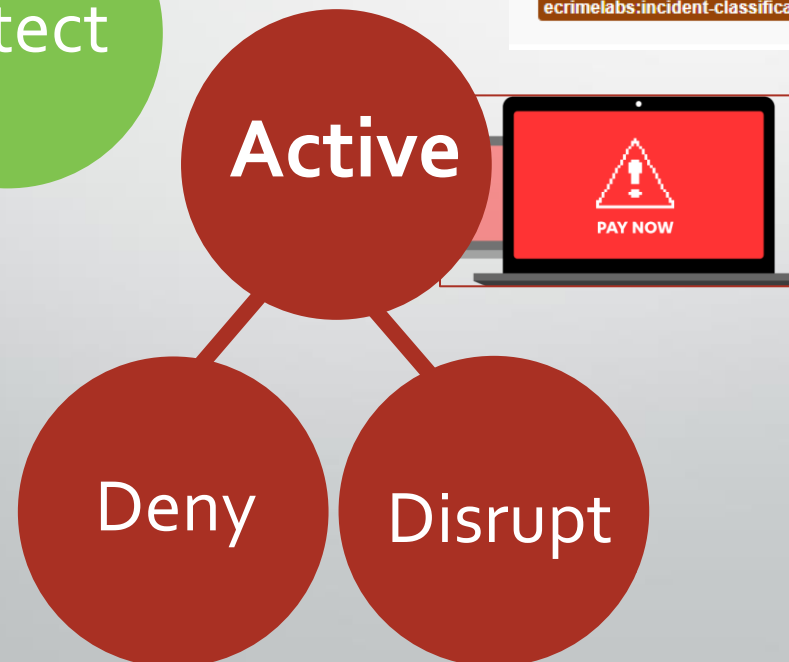


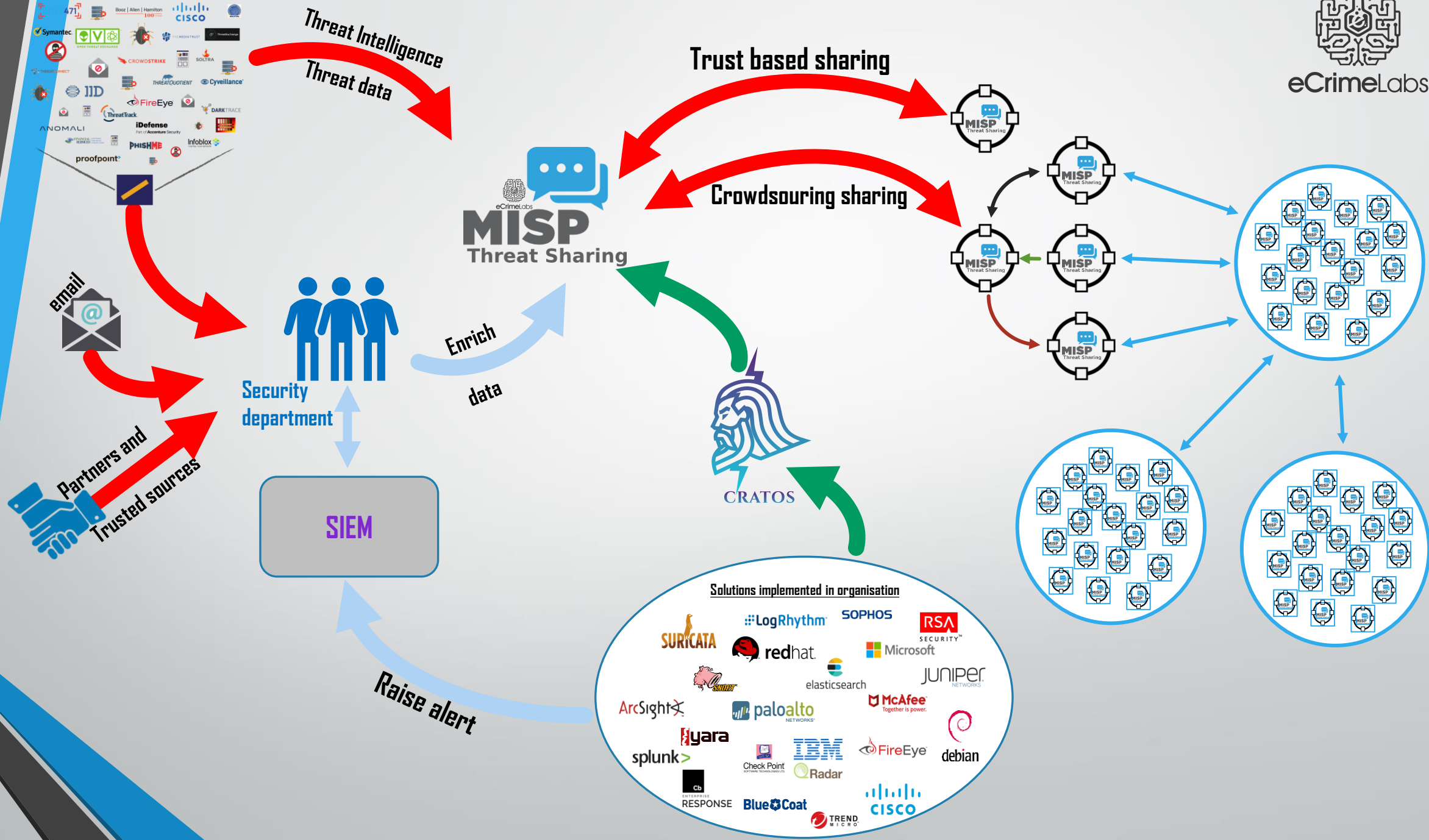
Download

Using the capabilities during an incident



Name ↓
ecrimelabs:incident-classification=alert
ecrimelabs:incident-classification=block
ecrimelabs:incident-classification=cust1
ecrimelabs:incident-classification=cust2
ecrimelabs:incident-classification=cust3
ecrimelabs:incident-classification=cust4
ecrimelabs:incident-classification=cust5
ecrimelabs:incident-classification=false-positive
ecrimelabs:incident-classification=hunt
ecrimelabs:incident-classification=incident





Future work

- Improve documentation
- Optimize the code, hopefully with the help of the community
- Add feature for minimizing the data even more (What feeds should be selectable)
- Add feature to for a token to query what events an indicator were seen, for more easy traceability.
- Add possibility for more complex outputs (Vendor solution specific)
- Release it as stable version.
- Continue improvements and add features while still keeping it light-weight.



Try it out during Hack.lu
Token will expire within two weeks
<https://www.evilcorp.dk/hacklu.txt>



Questions

<https://github.com/eCrimeLabs/cratos-fastapi>

Review Release

Need some public code review

Disclaimer:

#ImNotADeveloper



<https://www.ecrimelabs.com>



@DennisRand
@eCrimelabs