



HACK.LU 2019 / 2019-10-24

PRACTICAL INCIDENT RESPONSE

WITH AUTOMATION AND COLLABORATION INSIDE

AGENDA

- ▶ TheHive & its Main Features
- ▶ Cortex & its Main Features
- ▶ Additional Definitions & Concepts
- ▶ Sharing
- ▶ A Typical Integration
- ▶ Clustering
- ▶ Going Further
- ▶ It's Your Turn!

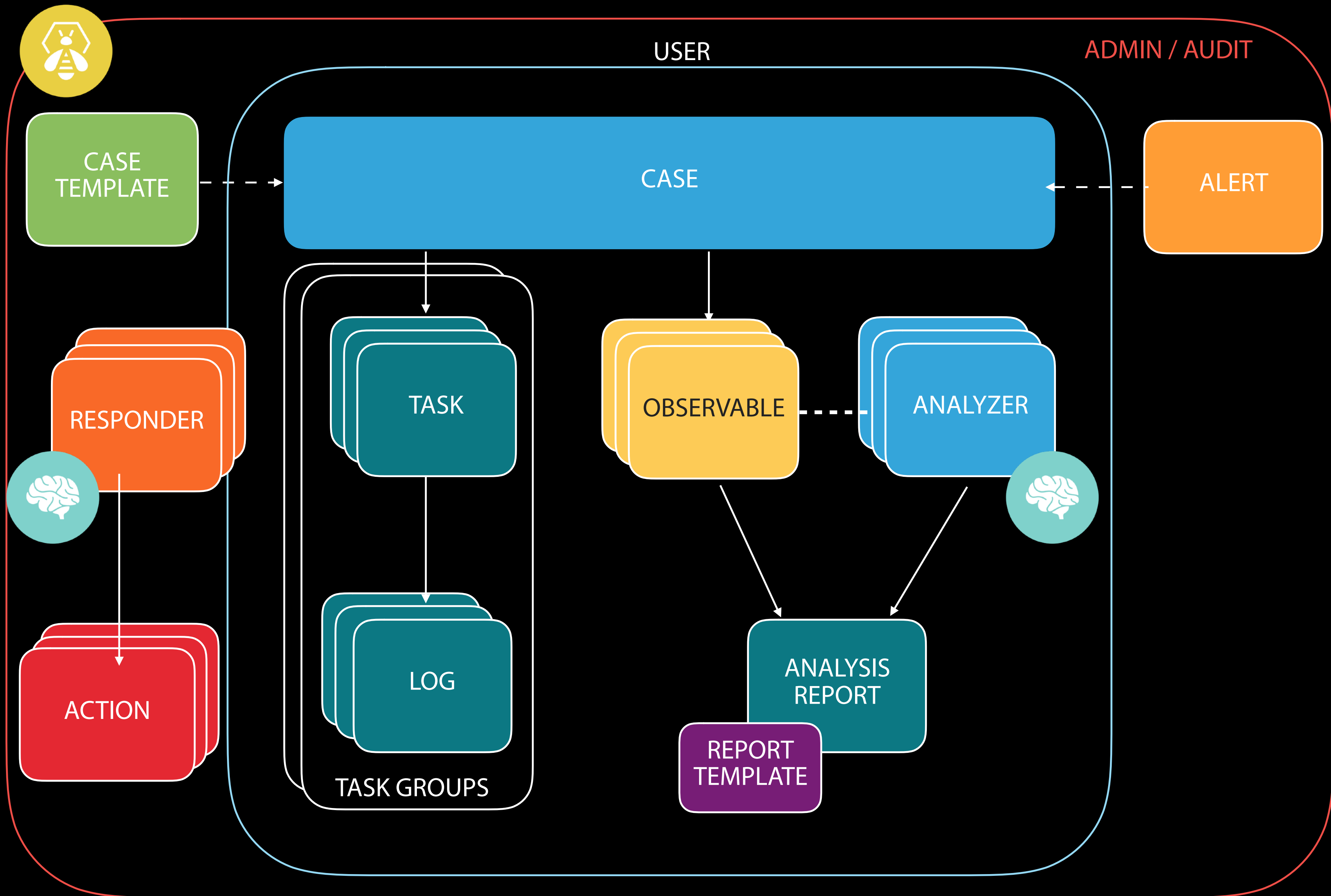


THEHIVE



- ▶ **SIRP / SOAR**
- ▶ **Collaborate** in real-time
 - ▶ Handle & respond to incidents
 - ▶ Perform forensics analysis
- ▶ **Organise**, structure and archive incidents
- ▶ **Corelate** & merge incidents
- ▶ Gather & **share** IOCs with communities (using the native MISP integration)

WORKFLOW





- ▶ Custom **case templates**: incident workflows
- ▶ Augment your processes with metrics & **custom fields**
- ▶ Generate fully customisable **dashboards**: track activity, follow KPIs...
- ▶ **Feeders**: get alerts from MISP, CTI providers, SIEM, emails, ...
- ▶ **Triage** & merge alerts
- ▶ Find **similarities** across cases & alerts
- ▶ Define observables as **IOCs** and/or **sighted**
- ▶ **Audit** trails
- ▶ REST **API**
- ▶ **Webhook** support



CORTEX



- ▶ Observable **analysis** & **active response** engine
- ▶ Analyze using the Web UI or through the REST API
- ▶ Respond & **take action**
- ▶ Use Python (or other languages supported by Linux) to write your own
- ▶ TheHive can leverage multiple Cortex instances
- ▶ Use MISP for additional analysis possibilities

120+
ANALYZERS





-
- ▶ **Multi-tenancy**: Manage users and groups (organisations)
 - ▶ Adjust **TLP** & **PAP** (Permissible Actions Protocol)
 - ▶ Jobs **history**
 - ▶ **Cache** jobs & reports
 - ▶ Custom **rate limiting** for each analyzer
 - ▶ Can use **Docker** to run analyzers and responders



ADDITIONAL CONCEPTS



- ▶ **Gather** information from an external service
 - ▶ Mail server
 - ▶ CTI provider
 - ▶ SIEM ...
- ▶ **Process** data and format for TheHive
 - ▶ TheHive uses Markdown text formatting
- ▶ **Import** data as Case or Alert



- ▶ **Automatic** action triggered by an event
- ▶ TheHive can send all events to an external application
- ▶ This application can **trigger actions** on specific events
- ▶ Ex:
 - ▶ Create a ticket when a specific tag is added to a Case
 - ▶ Run Analyzers X and Y on an observables when the Alert is converted as a Case



- ▶ **Metric:** numerical information
 - ▶ Ex: number of malicious emails that were delivered
- ▶ **Custom Field:** additional information, useful for giving more context
 - ▶ Ex: targeted Business Unit
- ▶ **Case Template:** workflow of tasks and default metadata (playbook)
 - ▶ Can contain metrics and custom fields
 - ▶ Create a case from a template
 - ▶ Import an alert and apply a template



- ▶ Programs for **processing observables** and **delivering reports**
- ▶ Input: observable + metadata
- ▶ Output:
 - ▶ Summary report
 - ▶ Long report
 - ▶ Observables (optional)
- ▶ Ex: get the VirusTotal report for a given hash/file



- ▶ Programs to **take action** at the Alert, Case, Task, Log or Observable level
- ▶ Input: data and metadata
- ▶ Output: Success Failure
 - ▶ Operations : ex: "Add tag in case", "Add tag in Observables"
- ▶ Mostly **customer-specific**
- ▶ Ex.
 - ▶ Block a set of malicious URLs
 - ▶ Reply to a user notification

EVENTS

List of alerts (179 of 178)

No event selected ▾ Quick Filters ▾ Sort by ▾ Stats Filters 15 per page

1 filter(s) applied: Status: New, Updated ✕ Clear filters

First Previous 1 2 3 4 5 ... Next Last

<input type="checkbox"/>	Reference	Type	Status	Title	Source	Severity	Attributes	Date			
<input type="checkbox"/>	488	misp	New	#488 [Malspam] Sixt Invoice: 5759752410 src:TRAINING	MISP-HONEYLOVE	M	9	Sun, Oct 14th, 2018 20:35 +02:00			
<input type="checkbox"/>	486	misp	New	#486 OSINT (expanded) - Xbash Combines Botnet, Ransomware, Coinmining in Worm t hat Targets Linux and Windows src:CIRCL ms-caro-malware:malware-platform="Python" osint:source-type="blog-post" misp-galaxy:mitre-enterprise-attack-attack-pattern="Exploit Public-Facing Application - T1190" misp-galaxy:mitre-enterprise-attack-attack-pattern="Standard Application Layer Protocol - T1071" misp-galaxy:tool="Xbash" misp-galaxy:threat-actor="Iron Group"	MISP-HONEYLOVE	L	133	Sun, Oct 14th, 2018 20:35 +02:00			
<input type="checkbox"/>	485	misp	New	#485 OSINT - Dangerous Invoices and Dangerous Infrastructure src:CIRCL osint:source-type="blog-post" estimative-language:confidence-in-analytic-judgment="moderate"	MISP-HONEYLOVE	L	41	Sun, Oct 14th, 2018 20:35 +02:00			
<input type="checkbox"/>	484	misp	New	#484 OSINT - Multi-exploit IoT/Linux Botnets Mirai and Gafgyt Target Apache Struts, Son icWall	MISP-HONEYLOVE	L	143	Sun, Oct 14th, 2018 20:35 +02:00			

L #485 OSINT - Dangerous Invoices and Dangerous Infrastructure

Date: Sun, Oct 14th, 2018 20:35 +02:00 **Type:** misp **Reference:** 485 **Source:** MISP-HONEYLOVE

src:CIRCL **osint:**source-type="blog-post" **estimative-language:**confidence-in-analytic-judgment="moderate"

Description

Imported from MISP Event #485, created at Sun Oct 14 18:35:19 UTC 2018

Additional fields

No additional information have been specified

Observables (41)

All (41) other (20) hash (18) domain (1) url (1) ip (1)

Type	Data
other	21/66
other	hxxps://www[.]virustotal[.]com/file/aff30dd46fdbfa278e95e5958d1dd7ff0e525e5e4d3dc2b214a6ed267f27184f/analysis/1537147114/
hash	107e57389903e3ea717845570a9e68174cfff86f70ebfa5f0023236eb1fb3d46
other	2018-09-13 06:39:02
other	2018-09-17 01:18:34
other	44/68
other	hxxps://www[.]virustotal[.]com/file/1c1e473d385b1c258f15d344ac5856fe88df88b1c477d9d8300e2981bb762525/analysis/1536820742/
hash	7b75837021f0271da96082239bd1ab650a5391919da7decc93ca03a7ae51899d
domain	rollboat[.]tk

Case template management

[+ New template](#)
[Import template](#)

Current templates

Generic Offense

Case basic information

Template name *
This name should be unique

Title prefix
This is used to prefix the case name

Severity M
This will be the default case severity

TLP TLP:AMBER
This will be the default case TLP

PAP PAP:AMBER
This will be the default case PAP

Tags
These will be the default case tags

Description *

[Delete case template](#) * Required field

Tasks (10)

- [Generic] Scratchpad [Edit](#) [Delete](#)
- [Identification] Initial Assessment [Edit](#) [Delete](#)
- [Identification] In-Depth Analysis [Edit](#) [Delete](#)
- [Generic] Containment [Edit](#) [Delete](#)
- [Generic] Eradication [Edit](#) [Delete](#)
- [Generic] Recovery [Edit](#) [Delete](#)
- [Generic] Lessons Learned [Edit](#) [Delete](#)
- [Communication] Internal [Edit](#) [Delete](#)
- [Communication] Peers & Partners [Edit](#) [Delete](#)
- [Communication] Other [Edit](#) [Delete](#)

Metrics (0)

No metrics have been added. [Add a metric](#)

Custom fields (0)

No custom fields have been added. [Add a custom field](#)

[Export case template](#) [+ Save case template](#)

other

2018-09-16 00:10:47

Cancel

✉ Mark as read

👁 Ignore new updates

Import alert as

MISP-EVENT

Yes, Import

Case # 2 - [MISP] #485 OSINT - Dangerous Invoices and Dangerous Infrastructure

Created by Saâd Kadhi Mon, Oct 15th, 2018 10:11 +02:00

Close Flag Merge Remove | Share (1) | Responders

Details

Tasks 10

Observables 41

Summary

Title [MISP] #485 OSINT - Dangerous Invoices and Dangerous Infrastructure

Severity L

TLP TLP:WHITE

PAP PAP:AMBER

Assignee Saâd Kadhi

Date Sun, Oct 14th, 2018 20:35 +02:00

Tags estimative-language:confidence-in-analytic-judgment="moderate"
osint:source-type="blog-post" src:CIRCL misp-event

Additional information

No additional information have been specified

Metrics

No metrics have been set

Description

Imported from MISP Event #485, created at Sun Oct 14 18:35:19 UTC 2018

Open in new window Hide

Added by Saâd Kadhi a few seconds

[MISP] #485 OSINT - Dangerous Invoices and Dangerous Infrastructure

This case contains 10 tasks [See all](#)

This case contains 41 observables [See all](#)

description: Imported from MISP Event #485, created at Sun Oct 14 18:35:19 UTC 2018

#2 - [MISP] #485 OSINT - Dangerous Invoices and Dangerous Infrastructure

Details Tasks **10** Observables **41**

Action **+ Add observable(s)** **Stats** **Filters** 15 per page

Statistics

Observables by type

other	20
hash	18
domain	1
url	1
ip	1

Observables as IOC

Not IOC	41
---------	----

Top 10 tags

MISP:type=link	7
MISP:type=text	7
MISP:type=sha256	6
MISP:type=datetime	6
MISP:type=md5	6
MISP:type=sha1	6
MISP:category=Network activity	3
MISP:type=url	1
MISP:type=domain	1
MISP:type=ip-src	1

Observable List (41 of 41)

First Previous **1** 2 3 Next Last

<input type="checkbox"/>	Type	Value/Filename	Date Added	Actions
<input type="checkbox"/>	other	hxxps://www[.]virustotal[.]com/file/7b75837021f0271da96082239bd1ab650a5391919da7decc93ca03a7ae51899d/analysis/1537146697/ MISP:type=link MISP:category=External analysis src:MISP-HONEYLOVE misp-honeylove No reports available	09/17/18 7:26	

Case # 2 - [MISP] #485 OSINT - Dangerous Invoices and Dangerous Infrastructure

Created by Saâd Kadhi Mon, Oct 15th, 2018 10:11 +02:00 **1 Related case** Close Flag Merge Remove | Share (1) | Responders

Details Tasks **10** Observables **42** **+1**

Summary

Title [MISP] #485 OSINT - Dangerous Invoices and Dangerous Infrastructure

Severity L

TLP TLP:WHITE

PAP PAP:AMBER

Assignee Saâd Kadhi

Date Sun, Oct 14th, 2018 20:35 +02:00

Tags estimative-language:confidence-in-analytic-judgment="moderate"
osint:source-type="blog-post" src:CIRCL misp-event

Related cases

Newest (Case # 1 - [Generic Offense] Contact from Suspicious IP 171.223.130.224)

Created on **2018-10-12**

Shares **1 observable (1 IOC)**

Tagged as offense generic alert

See all (1 related case)

Seen elsewhere

ONTO ANALYSIS

Action ▾ **+ Add observable(s)** 1 observable(s) selected Stats Filters 15 per page

- Export
- Change sighted flag
- Change IOC flag (42)
- Change TLP
- Add tag
- Run analyzers**
- Delete

First Previous **1** 2 3 Next Last

<input type="checkbox"/>	Type ▾	Value/Filename ⇅	Date Added ▾	Actions
<input checked="" type="checkbox"/>	ip	171[.]223[.]130[.]224 MISP:type=ip-dst MISP:category=Network activity src:MISP-HONEYLOVE misp-honeylove No reports available	10/14/18 22:49	

ONTO ANALYSIS

Run analyzers ▾ **+ Add observable(s)** 1 observable(s) selected Stats Filters 15 per page






Select All Deselect All

- Abuse_Finder_2_0
- CyberCrime-Tracker_1_0
- DShield_lookup_1_0
- DomainTools_ReverseIP_2_0
- DomainTools_ReverseWhois_2_0
- DomainTools_WhoisLookup_IP_2_0
- MaxMind_GeoIP_3_0
- VirusTotal_GetReport_3_0

Run selected analyzers Cancel

Observable List (42 of 42)

First Previous **1** 2 3 Next Last

<input type="checkbox"/>	Type ↕	Value/Filename ↕	Date Added ▾	Actions
<input checked="" type="checkbox"/>	 ip	171[.]223[.]130[.]224  MISP:type=ip-dst  MISP:category=Network activity  src:MISP-HONEYLOVE  misp-honeylove	10/14/18 22:49	

ONTO ANALYSIS

Open in new window Hide

+ Added by Saâd Kadhi a few seconds

⚙️ **Job: DShield_lookup_1_0 started**

startDate: Mon, Oct 15th, 2018 10:27 +02:00

status: InProgress

📁 #2 - [MISP] #485 OSINT - Dangerous Invoices and Dangerous Infrastructure ↗ 171.223.130.224

👁 ip

171[.]223[.]130[.]224

🔑 MISP:type=ip-dst MISP:category=Network activity src:MISP-HONEYLOVE misp-honeylove

⚙️ DShield:Score="1670 count(s) / 1589 attack(s) / 1 threatfeed(s)" VT:Score="0"

Report for DShield_lookup_1_0 analysis of Mon, Oct 15th, 2018 10:28 +02:00

Show Raw Report Show observables (2)

DShield IP Reputation Summary

IP: 171.223.130.224
Reputation: Malicious
Network: 171.208.0.0/12
AS: 4134
AS Name: CHINANET-BACKBONE No.31,Jin-rong Street,
AS Country: CN
AS Abuse Contact: anti-spam@ns.chinanet.cn.net
Number of Attacks: 1670
Unique Attacked Hosts: 1589
First Reported Attack: 2018-10-11
Last Reported Attacks: 2018-10-11
Risk Level: 6
Comment: None
Threat Feeds: 1

Threat Feeds

ciarmy First Seen: 2018-10-12



ONTO ANALYSIS

Report for DShield_lookup_1_0 analysis of Mon, Oct 15th, 2018 10:28 +02:00

[Show Raw Report](#) | [Hide observables \(2\)](#)

Observables Extracted from analysis report

[All \(2\)](#) [mail \(1\)](#) [autonomous-system \(1\)](#)


0 items selected [Select all](#)

	Type	Data
<input type="checkbox"/>	autonomous-system	4134
<input type="checkbox"/>	mail	anti-spam@ns[.]chinanet[.]cn[.]net



SHARING



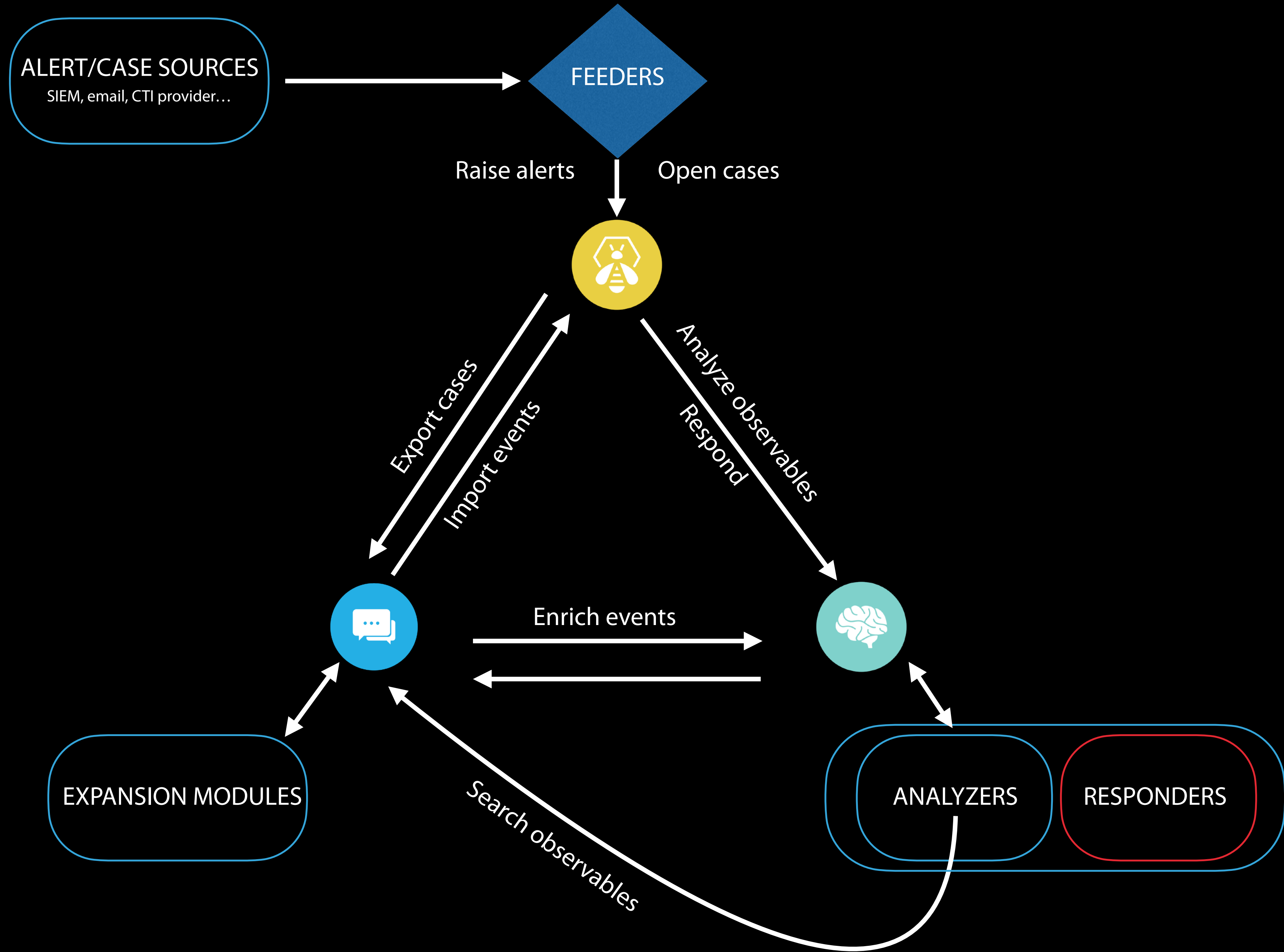
- ▶ TheHive only shares observables that are **IOCs**
- ▶ Prepare your case and **identify** observables that are IOCs
- ▶  **Share** the case
 - ▶ TheHive creates a new MISP event or extends an existing one
 - ▶ Title of the case is exported as title of event in MISP
 - ▶ IOCs in TheHive are exported as attributes in MISP
- ▶ TheHive **does not publish** the freshly created event



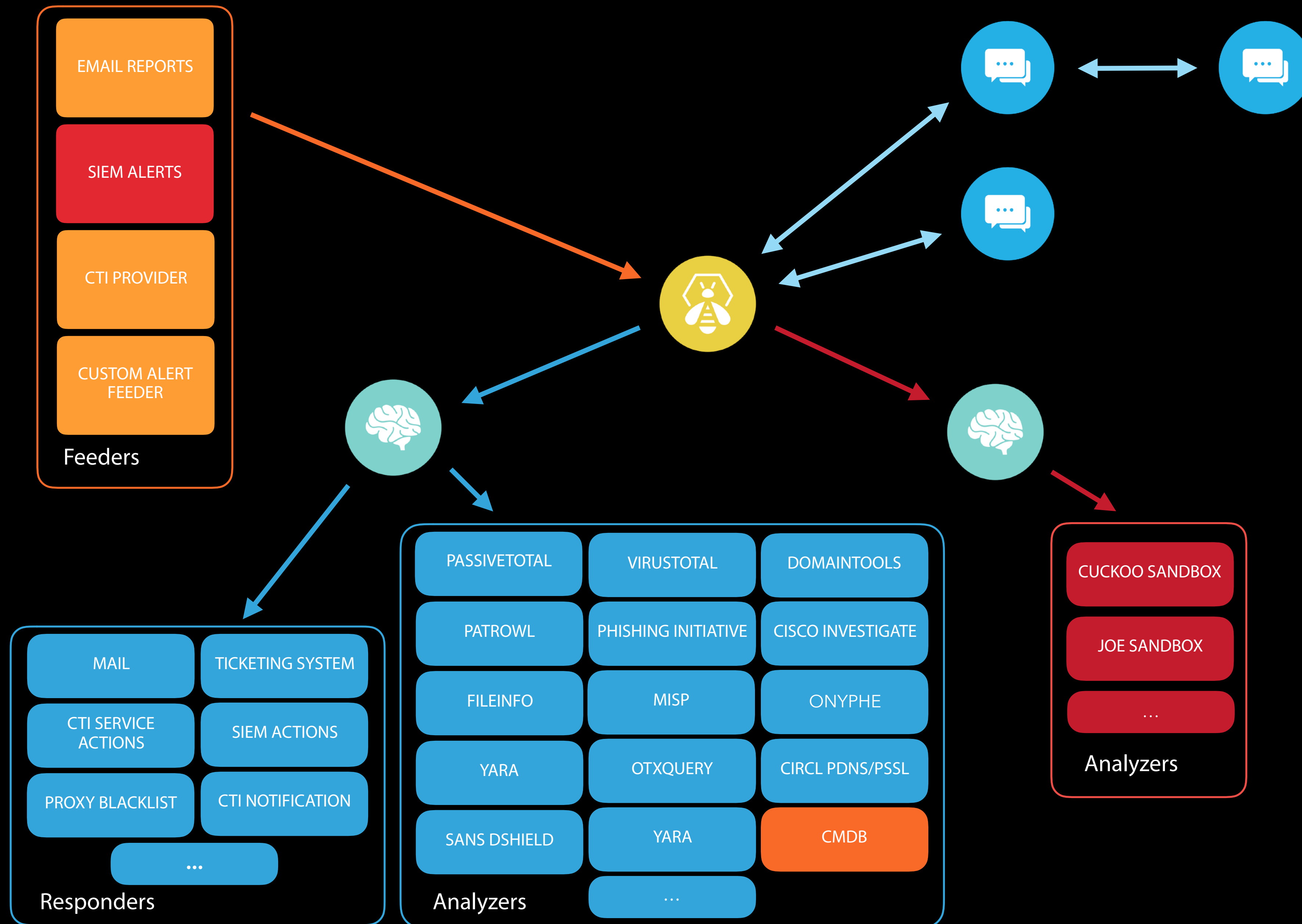
- ▶ Connect to MISP & review the new event
- ▶ **Update** the title & associated metadata
- ▶ **Review** the attributes & their datatypes
- ▶ **Enrich** with context, tags, taxonomies
- ▶ Identify **distribution lists** (communities, sharing groups)
- ▶ **Publish**



A TYPICAL INTEGRATION



REAL-WORLD EXAMPLE

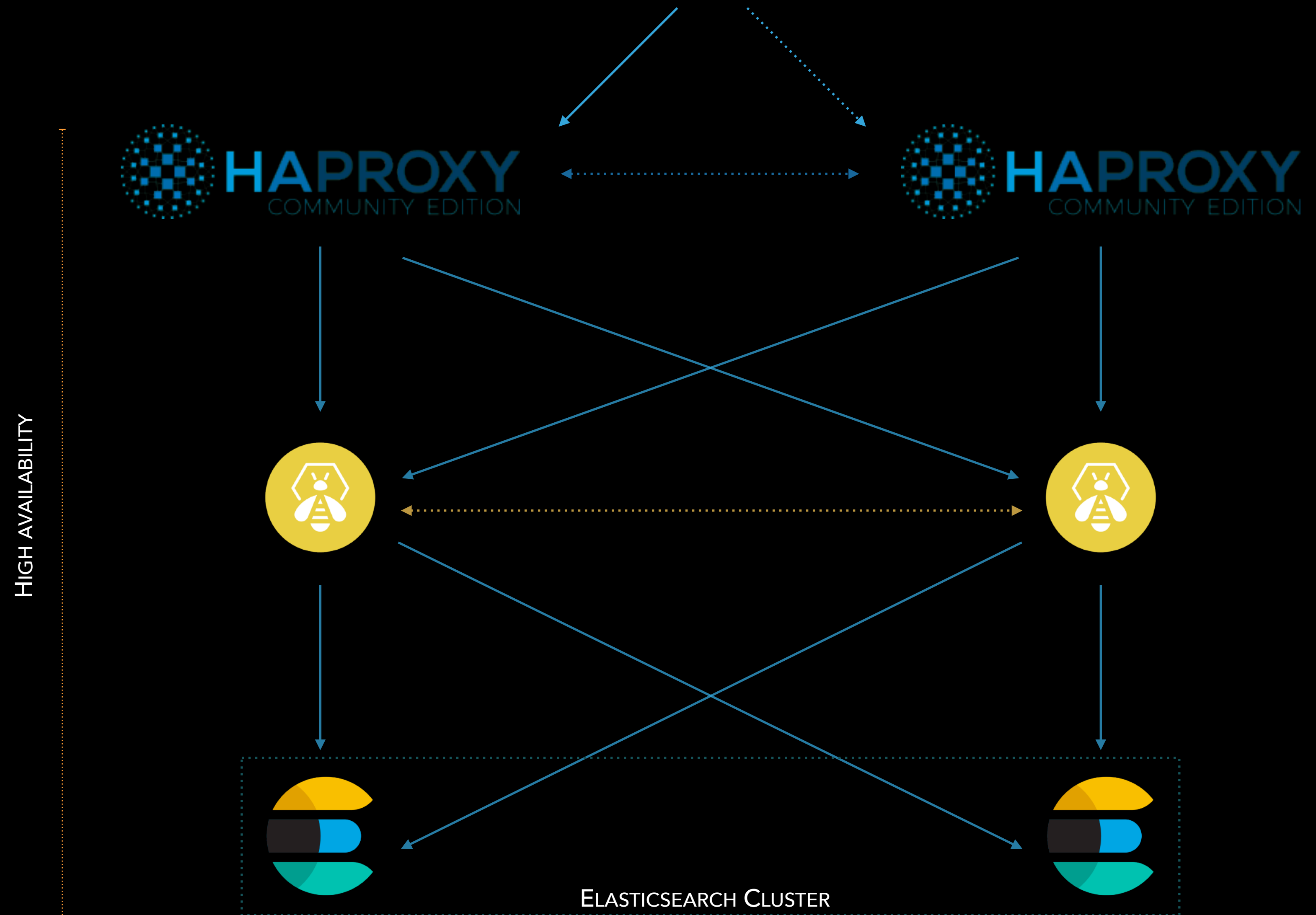




CLUSTERING

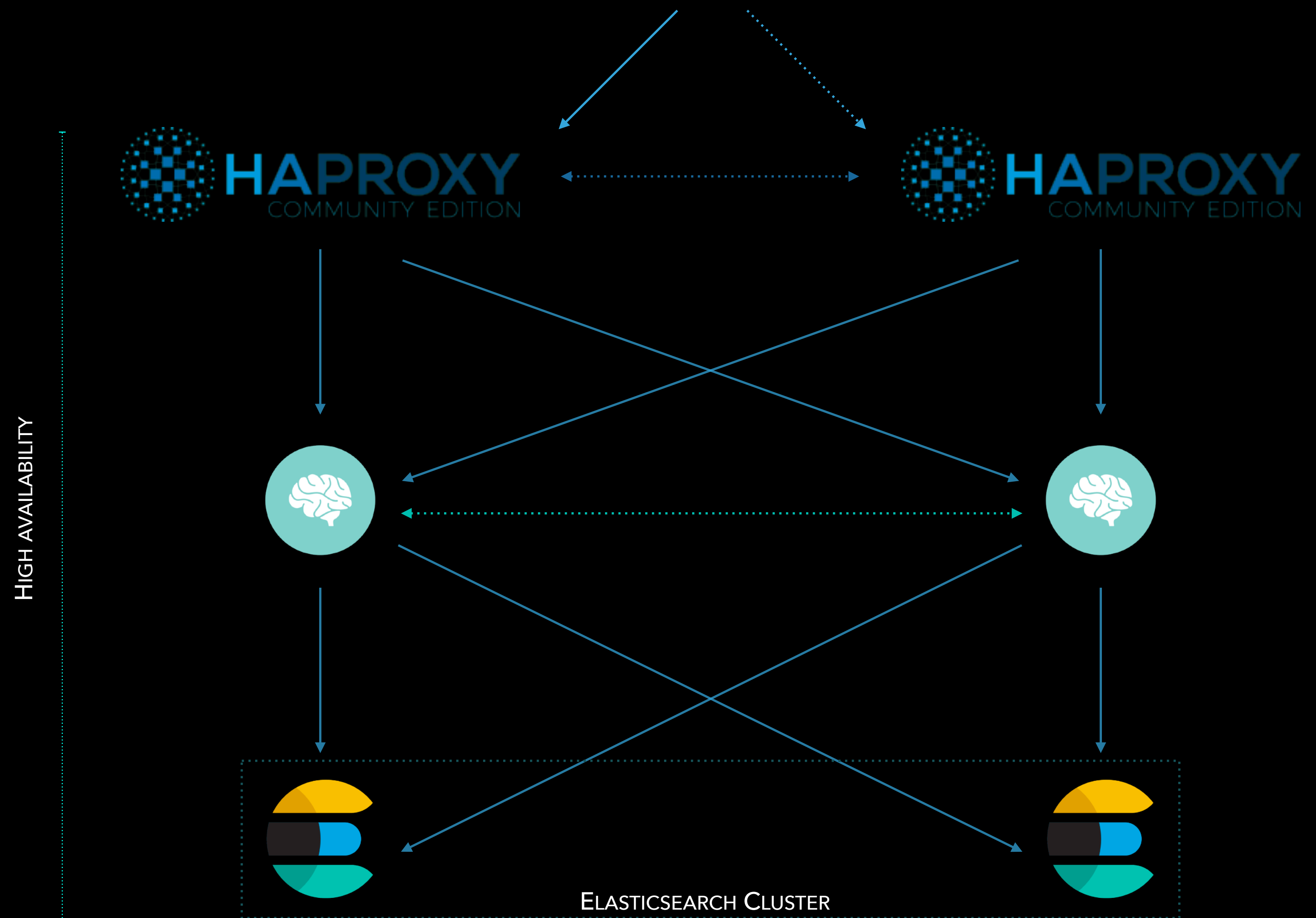
THEHIVE.MYDOMAIN.TLD

Virtual IP



CORTEX.MYDOMAIN.TLD

Virtual IP





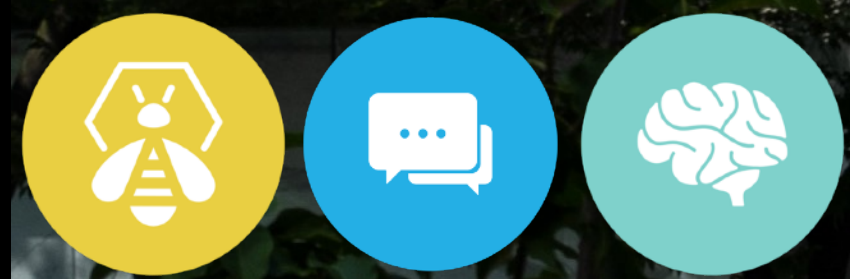
GOING FURTHER



- ▶ [TheHive4py](#), a REST API Python lib
- ▶ [Webhooks](#)
- ▶ Feeders: [Zerofox2TH](#), [DigitalShadows2TH](#), [FireEye2TH](#) ...
- ▶ [Training VM](#)
- ▶ [Analysis Information Leak Framework](#) by CIRCL with support for TheHive alert creation



- ▶ [Cortex4py](#), a REST API Python lib
- ▶ [Analyzers and Responders](#)
- ▶ [Cortexutils](#), a Python lib that facilitates analyzer & responder development



IT'S YOUR TURN!



If you are using Virtualbox, you will need to map the VM's port 9000 to localhost

Boot it & type in your browser: http://VM_IP:9000

username: **admin**
password: **thehive1234**

Get it from one of the USB sticks distributed by your friendly bees

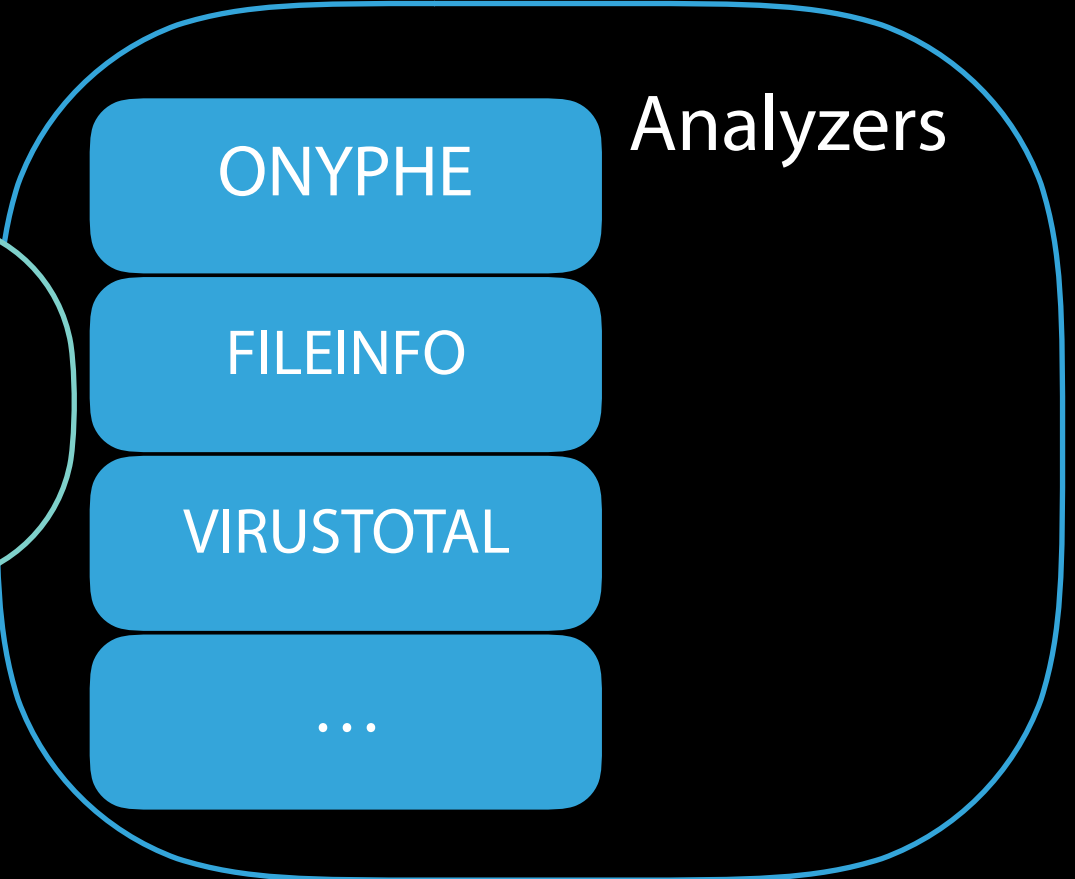
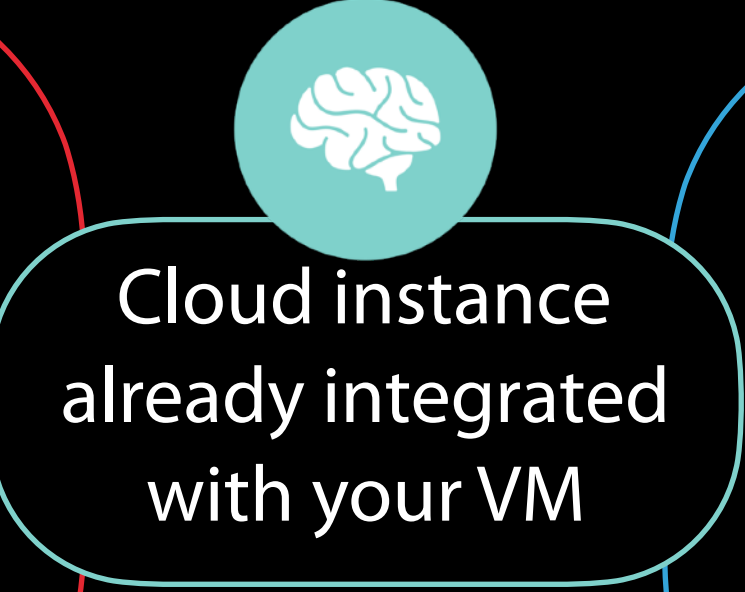
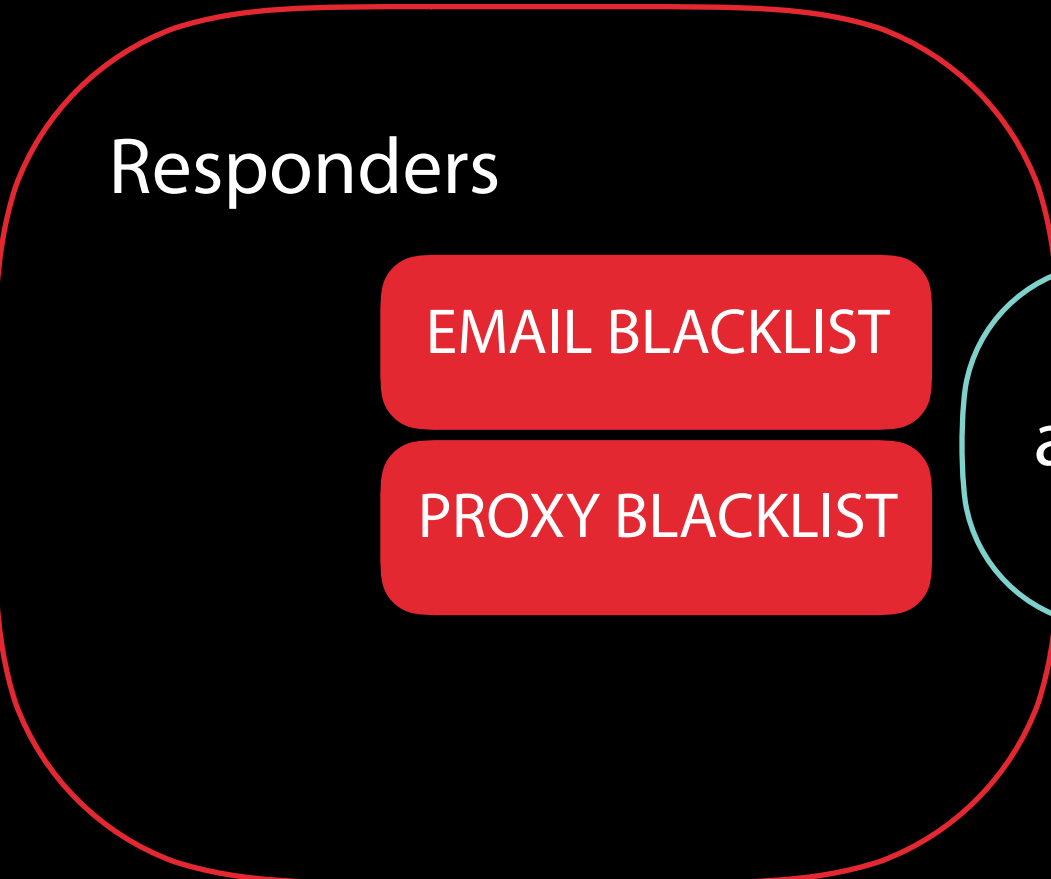
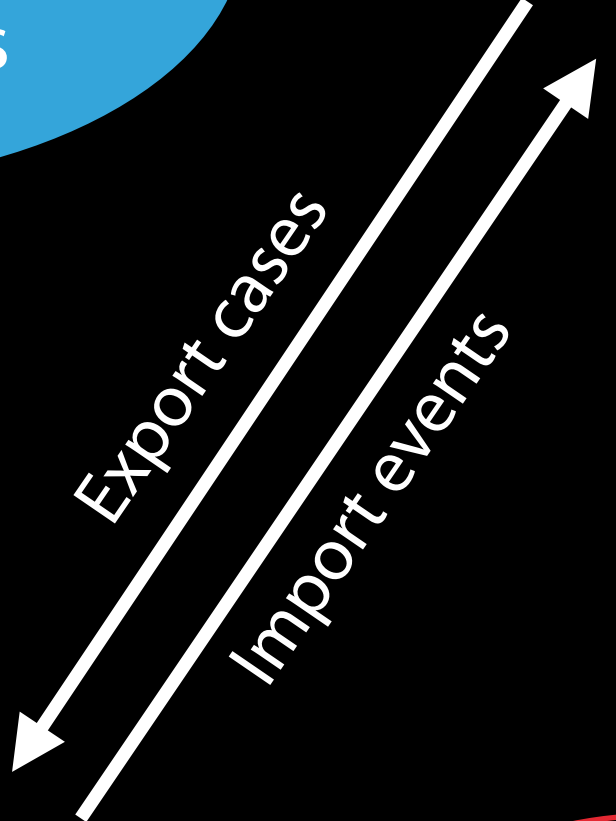


VERY IMPORTANT

Once you have logged in to the Web UI of TheHive, create a user **with read, write, admin roles** and **note it on the circulated sheet**

Use this new admin user from now on

It will have an important role



2 ALERTS TO INVESTIGATE

- ▶ Your workshop VM contains two alerts that need to be investigated
- ▶ **Import the first alert** (ALERT1). This will create a case with the observables from the alert
- ▶ **Try to come up with a workflow** and create tasks as you go to investigate
- ▶ Leverage Cortex analyzers and decide whether it is a true incident or not
- ▶ **If it is a true incident:**
 - ▶ Take action using Cortex responders
 - ▶ Tidy up your observables, mark those that you think are IOCs
 - ▶ Export your case to MISP
 - ▶ Complete all the tasks and close your case

TIME TO INVESTIGATE ALERT2

- ▶ **Before importing ALERT2**, preview it & decide what would be the **best workflow** to deal with similar alerts
- ▶ **Create a case template** corresponding to that workflow
 - ▶ Make sure that each task you create in the template is well defined (add a description to remember what needs to be done)
 - ▶ Hint: think of the SANS 6 steps incident response process
- ▶ Now import the alert as a case using the case template you've created
- ▶ Leverage Cortex analyzers and decide whether it is a true incident or not
- ▶ **If it is a true incident:**
 - ▶ Take action using Cortex responders
 - ▶ Tidy up your observables, mark those that you think are IOCs
 - ▶ Export your case to MISP

<https://thehive-project.org>

