



BSIDES LISBON / 2018-11-29

TLP:WHITE

CRUISING OCEAN THREAT WITHOUT SINKING

USING THEHIVE, CORTEX & MISP



OVERVIEW

THEHIVE PROJECT

GOALS

DRIVE THE TIME TO DETECT & REACT

CONTRIBUTE TO THE COMMUNITY

HOW

ALERT/EVENT COLLECTION

AUTOMATION

COLLABORATION



WHAT (TOOLS)

CYBER THREAT INTELLIGENCE

INCIDENT RESPONSE

DIGITAL FORENSICS

WHAT (TAKE TWO)



LIBRARIES

SYNAPSE

'FEEDERS'

WHO

THEHIVE CORE TEAM (6 MEMBERS)

A LARGE COMMUNITY (SOC/CSIRT/CERT)



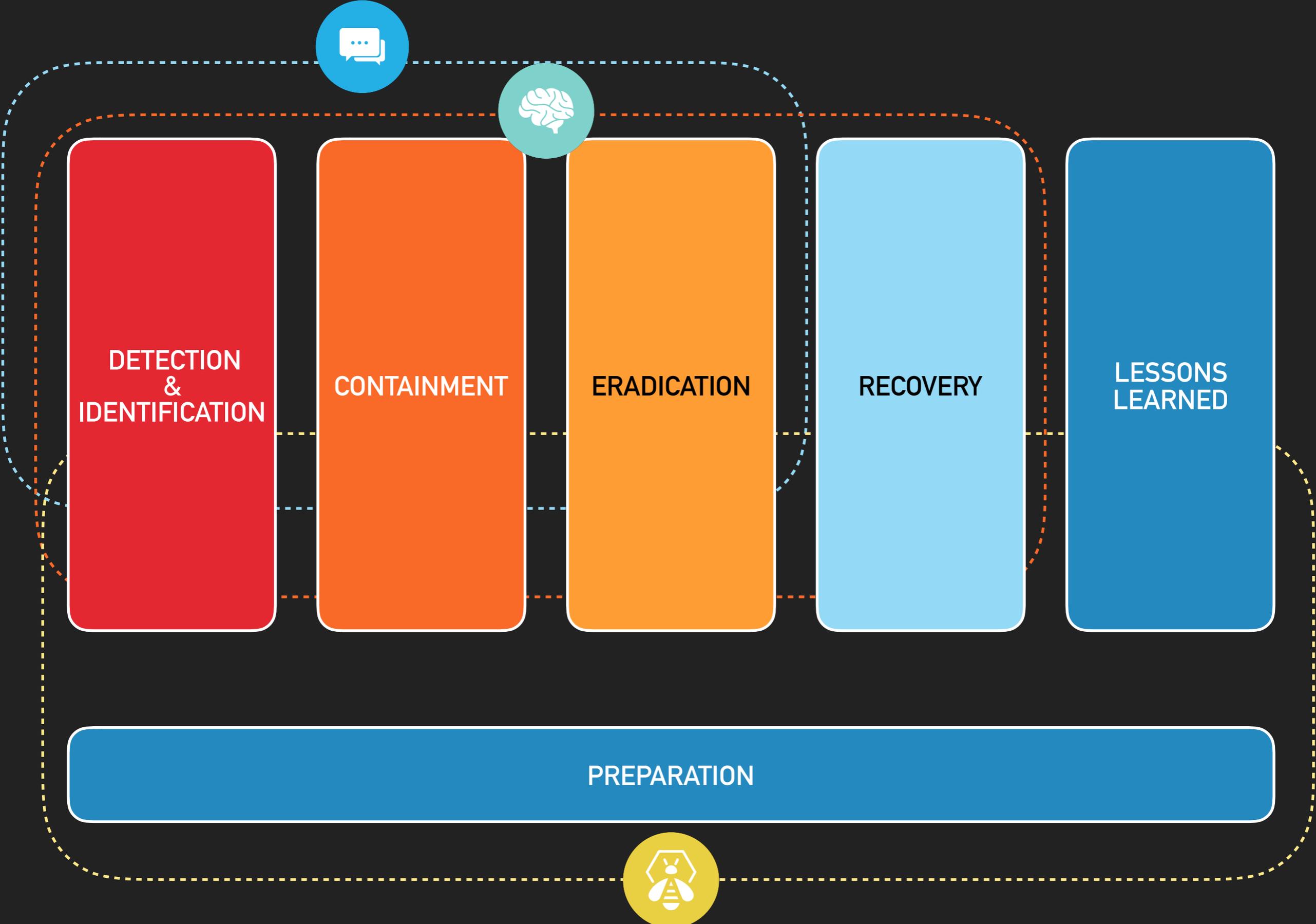
SINCE WHEN

OCT 2014 (PRIVATE VERSION)

NOV 2016 (FLOSS)

FEB 2017 (CORTEX)

WITHIN THE SANS 6 STEPS PROCESS



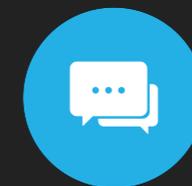


- ▶ **SIRP** / SOAR
- ▶ **collaborate** in real-time
- ▶ Fully customisable **dashboards** : track activity, follow KPIs...
- ▶ Use Cortex for at-scale **analysis** & active **response** 
- ▶ Leverage MISP for **CTI** functions 
- ▶ Multiple auth methods (LDAP, AD, OAuth 2, API keys...)
- ▶ **Webhook** support



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

101 ANALYZERS



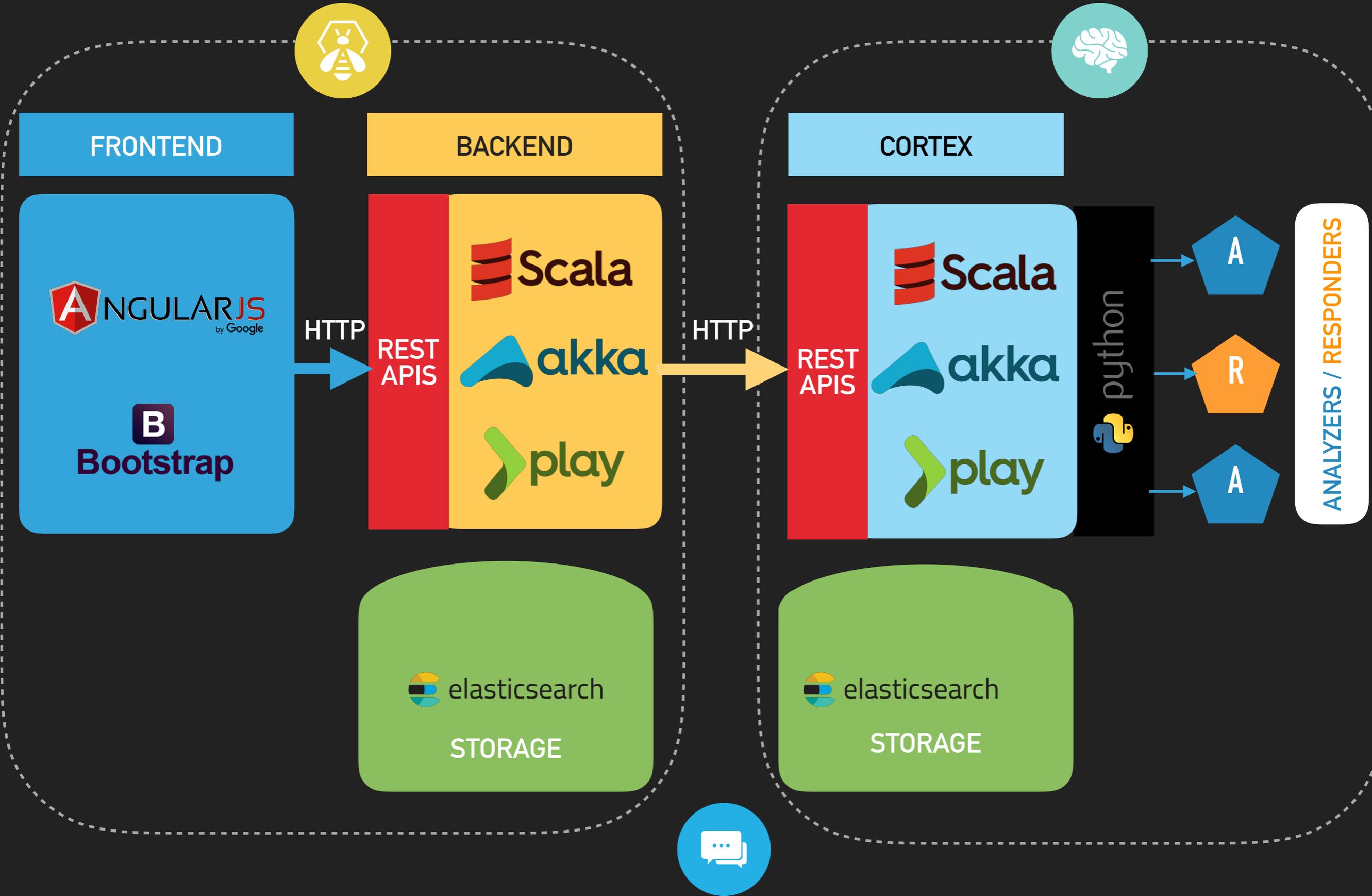


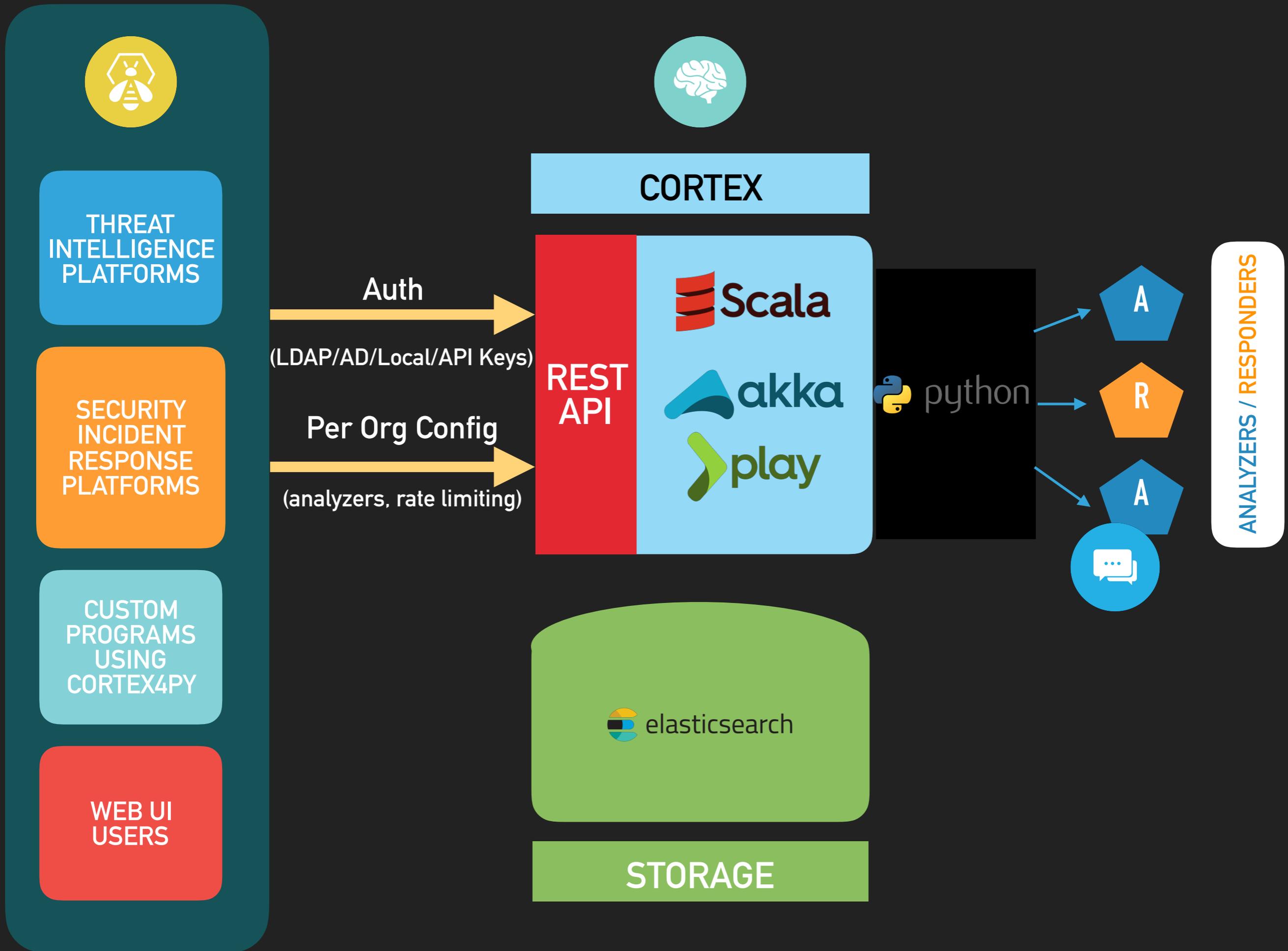
- ▶ The *de facto standard* for threat sharing
- ▶ Threat *intelligence* collection, sanitisation & dissemination
- ▶ Correlation & intelligence *storage*
- ▶ Supports tagging, galaxies, objects, taxonomies such as ATT&CK, & much more
- ▶ Can be highly *automated*
- ▶ TheHive can import from or export to multiple MISP instances
- ▶ Tightly integrated with Cortex for indicator *enrichment*

OR BOTH AT THE SAME TIME

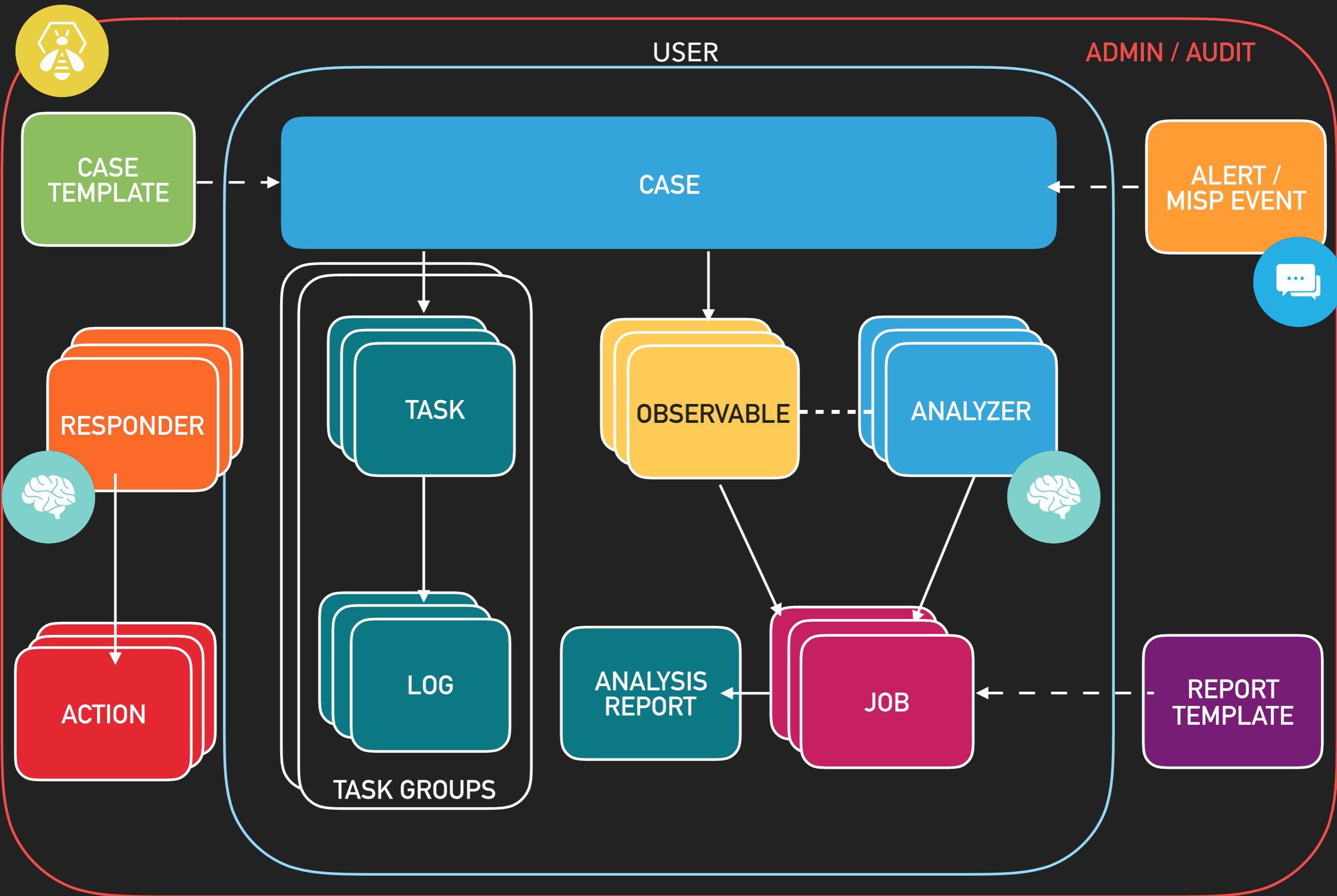


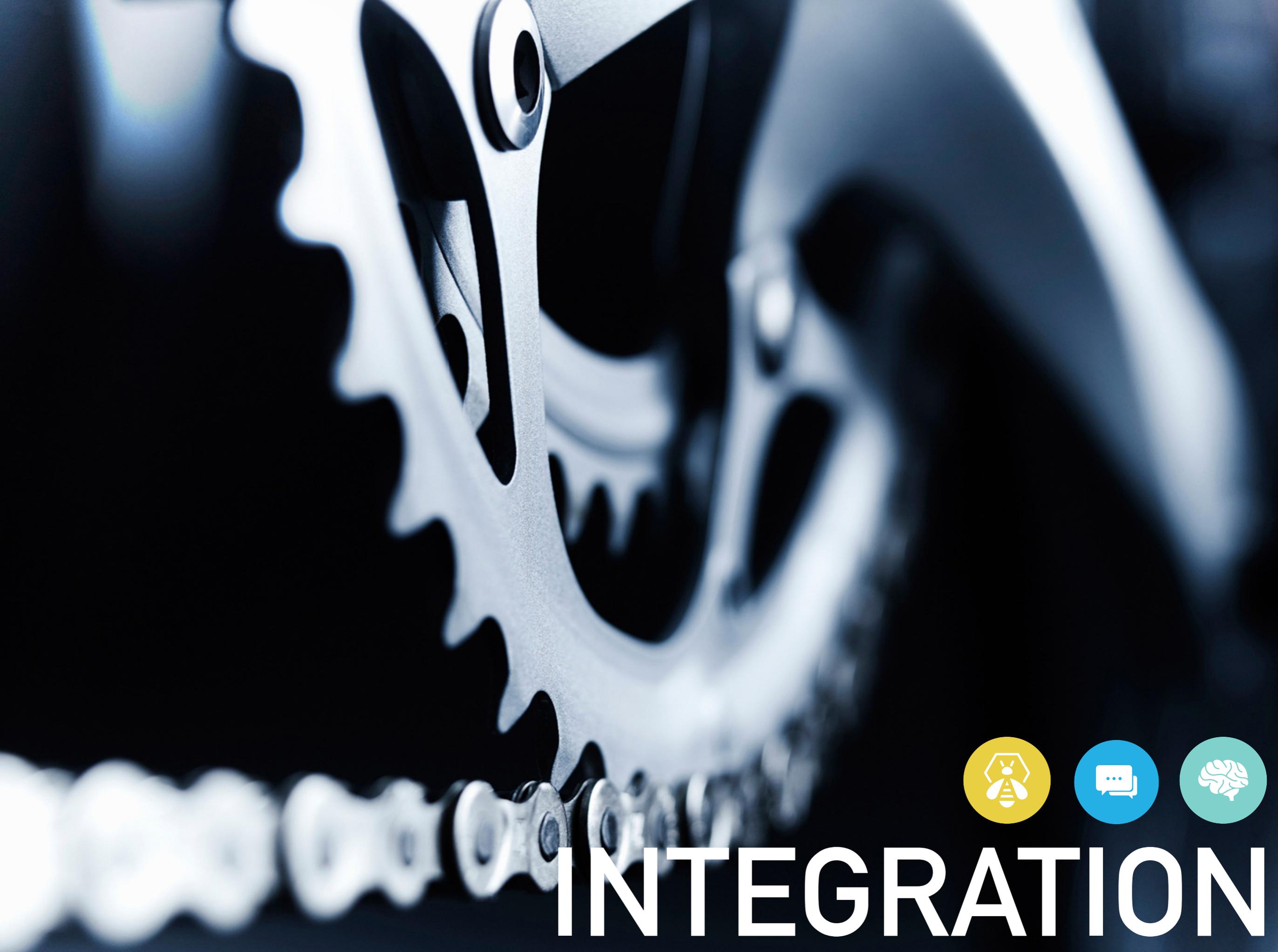
ARCHITECTURE



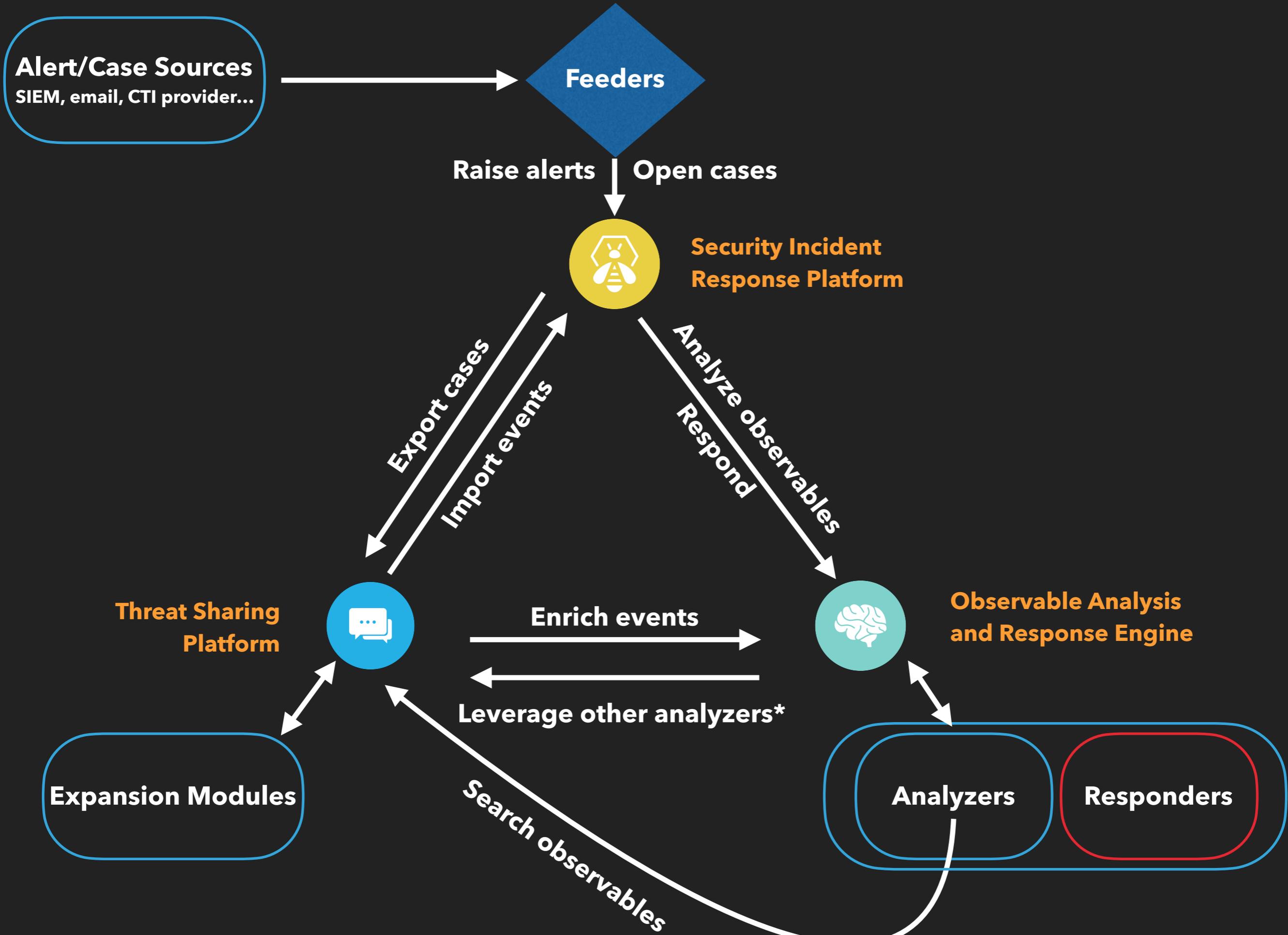


WORKFLOW





INTEGRATION



* Not supported currently in Cortex 2

SYNAPSE



EXCHANGELIB

EXCHANGE CONNECTOR

EWS2CASE WORKFLOW

QRADAR API

QRADAR CONNECTOR

QRADAR2ALERT WORKFLOW

THEHIVE CONNECTOR

THEHIVE4PY

API



EVENTS



+ New Case ▾

My tasks **0**

Waiting tasks **9**

Alerts **178**

Dashboards

Search

CaseId

Admin ▾



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	https://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	https://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 misp-event 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

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

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)

<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

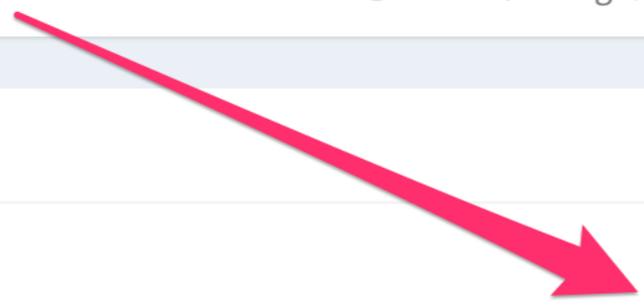
Newest (Case # 1 - [Generic Offense] Contact from Suspicious IP 171.223.130.224)

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
- Change TLP
- Add tag
- Run analyzers**

Delete

First Previous **1** 2 3 Next Last

type ▾

Value/Filename ⇅

Date Added ▾

Actions



ip

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

10/14/18 22:49



MISP:type=ip-dst

MISP:category=Network activity

src:MISP-HONEYLOVE

misp-honeylove



No reports available

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

MIND THE
INTERVAL (1H BY
DEFAULT)

AS LONG
AS YOU DON'T MERGE
CASES

- ▶ The MISP event used to create the case will **feed new observables** when new attributes are added to it
- ▶ When you add observables to your case during your investigation, only those flagged as IOCs can be shared back to the MISP event you used to create your case
- ▶ If its sync user cannot write to that event (different org for ex.), TheHive will create an [extended event](#)
- ▶ You can also **create a new event** on as many instances as you'd like

EXTENDED EVENTS

<input type="checkbox"/>	domain	stgg5jv6mqiibmax[.]torshop[.]li	10/15/18 10:46	
		suspicious		
		No reports available		
<input type="checkbox"/>	ip	171[.]223[.]130[.]224	10/14/18 22:49	
		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"		

Details Tasks 10 Observables 43 stgg5jv6mqiibmax[.]torsho

[DOMAIN]: stgg5jv6mqiibmax[.]torshop[.]li

Fortiguard:URLCat="Malicious Websites" VT:Score="3 detected_url(s)"

Metadata

TLP	TLP:AMBER
Date added	Mon, Oct 15th, 2018 10:46 +02:00
Is IOC	
Has been sighted	
Labels	suspicious
Description	 Suspicious activity going to this domain

EXTENDED EVENTS

MISP Export

You are about to export the case **[MISP] #485 OSINT - Dangerous Invoices and Dangerous Infrastructure** to one of the following MISP servers:

OK

MISP-HONEYLOVE

Export

Cancel

The case has been successfully exported with 1
observable(s) other 14/67

MISP:tv

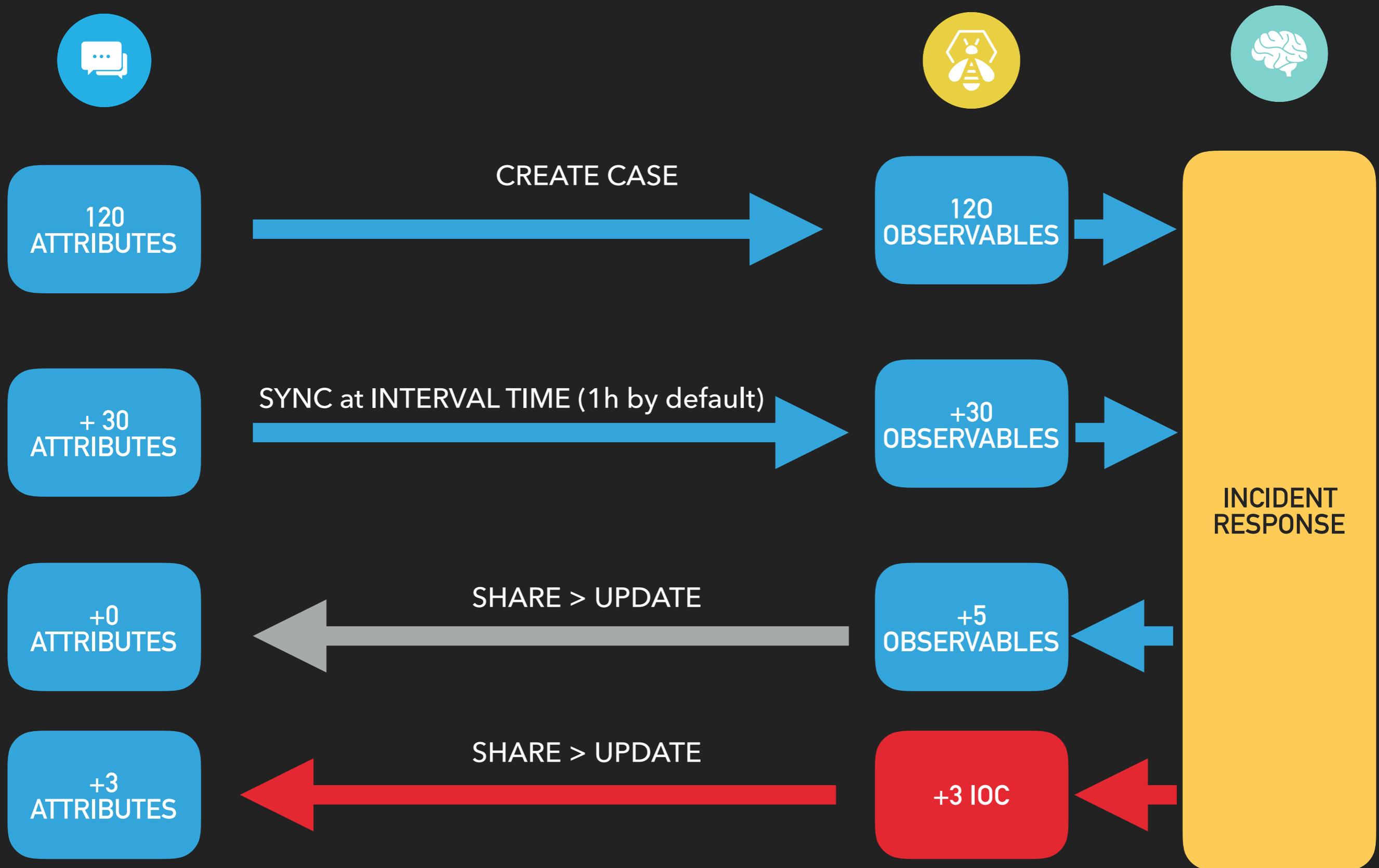
Published	Org	Owner Org	Id	Clusters	Tags	#Attr.	#Corr.	Email	Date	Info	Distribution	Actions
<input type="checkbox"/>		HONEYLOVE	HONEYLOVE	489	tlp:white	1		thehive@thehive.test	2018-10-14	[MISP] #485 OSINT - Dangerous Invoices and Dangerous Infrastructure	Organisation	
<input type="checkbox"/>	<input checked="" type="checkbox"/>		HONEYLOVE	485	tlp:white osint:source-type="blog-post" estimative-language:confidence-in-analytic-judgment="moderate"	53	1	admin@admin.test	2018-09-17	OSINT - Dangerous Invoices and Dangerous Infrastructure	All	

[MISP] #485 OSINT - Dangerous Invoices and Dangerous In...

Event ID	489
Uuid	5bc3b372-f8c0-4620-9613-289eac1063cf
Org	HONEYLOVE
Owner org	HONEYLOVE
Contributors	
Email	thehive@thehive.test
Tags	tlp:white
Date	2018-10-14
Threat Level	Low
Analysis	Initial
Distribution	Your organisation only
Info	[MISP] #485 OSINT - Dangerous Invoices and Dangerous Infrastructure
Published	No
#Attributes	1
Last change	2018-10-14 23:21:54
Extends	Event (485): OSINT - Dangerous Invoices and Dangerous Infrastructure
Extended by	
Sightings	0 (0) - restricted to own organisation only.
Activity	

Date	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings
<input type="checkbox"/>				2018-10-14	Network activity domain	stgg5jv6mqiibmax.torshop.li	tlp:amber Add	Suspicious activity going to this domain	<input checked="" type="checkbox"/>		Yes	Inherit	(0/0/0)

MISP & THEHIVE



BUT THERE'S MORE TO IT



- ▶ TheHive can monitor the **connection 'health'** of all the MISP and Cortex instances it is connected with 
- ▶ You can tailor MISP settings in TheHive in several ways



MAX ATTRIBUTES
PER EVENT

AGE OF THE LAST
PUBLICATION DATE

TAG WHITELIST*

TAG BLACKLIST

ORG BLACKLIST

MAX JSON SIZE

IMPORT/EXPORT/
(OR BOTH)

UPCOMING FEATURES

- ▶ TheHive 4.1 ~ Q2 2019
 - ▶ Replace Elasticsearch with a **GraphDB**
 - ▶ Share **sightings** with MISP
 - ▶ Add support for **MISP objects**
- ▶ TheHive 4.3 ~ Q4 2019
 - ▶ Add **taxonomy** (such as ATT&CK) support



TRY THE TRIO



-
- ▶ [TheHive](#), [Cortex](#) and [MISP](#) are available under a, free, open source **AGPLv3** license
 - ▶ TheHive and Cortex can be installed using **RPM**, **DEB**, **Docker** image, **binary** package or built from the **source** code
 - ▶ MISP can be installed using **Vagrant**, **VM**, **Docker** image or built from the **source** code
 - ▶ You can try TheHive, Cortex & MISP using the **training** VMs
 - ▶ **NEW**: [combined training VM](#) with TheHive, Cortex and MISP

ADDITIONAL SOFTWARE FROM THEHIVE PROJECT & MISP PROJECT

- ▶ [AIL](#) - Analysis Information Leak Framework by CIRCL with support for TheHive alert creation
- ▶ [TheHive4Py](#) - Python lib to create alert/case from multiple sources
- ▶ [Cortex4py](#) - Python lib to submit observables in bulk mode through the Cortex REST API from alternative SIRP platforms & custom scripts
- ▶ [DigitalShadows2TH](#) - TheHive Alert Feeder for Digital Shadows
- ▶ [Zerofox2TH](#) - TheHive Alert Feeder for Zerofox
- ▶ [Synapse](#) - Meta Alert Feeder with custom workflows. Currently supports Exchange, O365 & QRadar

ADDITIONAL SOFTWARE FROM THE COMMUNITY

- ▶ [FireEye2TH](#) - FireEye iSIGHT Alert Feeder for TheHive by LDO-CERT
- ▶ [Elastalert Hive Alerter](#) - use a custom Elastalert Alert to create alerts. contributed by Nclose
- ▶ [Email Feeder](#) - feed emails as alerts to TheHive, contributed by Xavier Mertens (SANS ISC)
- ▶ [qradar2thehive](#) - automatically create cases out of QRadar offenses, contributed by Pierre Barlet
- ▶ [TheHive DXL Python Service](#) - Access TheHive API via the Data Exchange fabric
- ▶ [Go-cortex-analyzers](#) - Additional analyzers written in GO by Rostelecom CERT

THANK YOU FOR YOUR ATTENTION
SEE YOU NEXT WEEK AT [BOTCONF](#) & THE WEEK AFTER AT [CIRCL](#)

