



FIRST CONFERENCE 29 / 2017-06-15

TLP:WHITE

A SCALABLE, OPEN SOURCE AND FREE INCIDENT RESPONSE PLATFORM

Saâd Kadhi

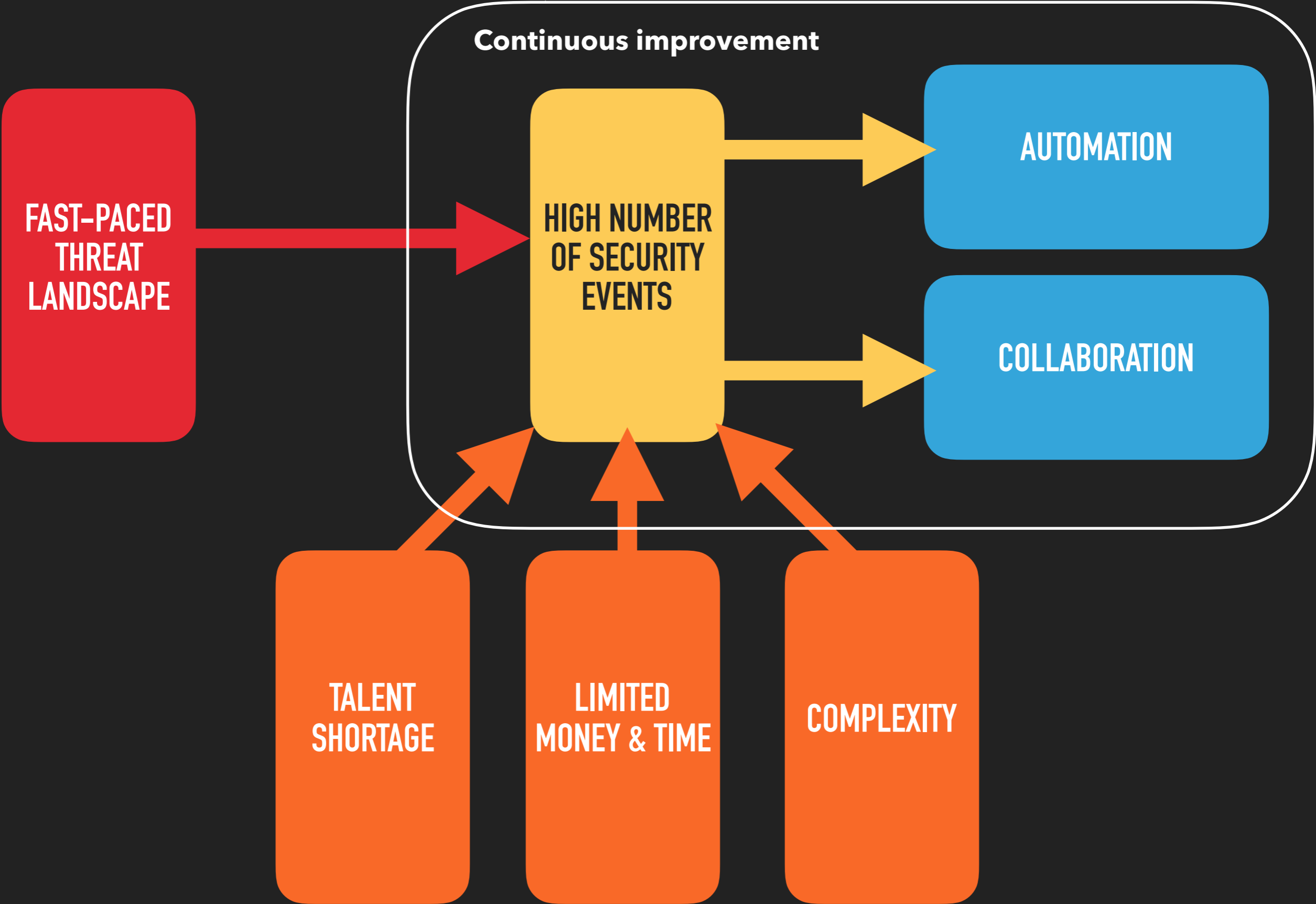
[CERT-BDF](#) / [TheHive Project](#)



THREATS & REACTION

OBSERVATIONS

DRIVING DOWN THE TIME TO REACT



DFIR = TEAM WORK

- ▶ DFIR = **team** work
- ▶ Mantra: 'with enough eyeballs, skills and mindsets, all threats are shallow'
- ▶ We shall seek to **drive** DFIR activity and continuously **improve** it
- ▶ Thanks to operational, meaningful **statistics**

SHARING IS CARING

- ▶ Investigation performed, IOCs **collected** and proper response done
- ▶ Wouldn't they be **useful** to **peers** to defend themselves?
- ▶ Hopefully, they will come up with **complementary** IOCs that were unbeknownst to us



HUNTING FOR A SOLUTION

SPECS

- ▶ Let many analysts **work** on multiple cases, sometimes **simultaneously**
- ▶ Collect observables and make their **analysis** as **simple** as possible
- ▶ **Index** observables, cases and any noteworthy evidence or reference

AUTOMATION & COLLABORATION

- ▶ Maintain **history** & an audit **trail**
- ▶ Change behavior according to the **TLP**
- ▶ Offer open, documented **API** to extract IOCs or create cases out of **MISP** events, **email** reports or **SIEM** alerts
- ▶ Generate statistics to drive and **improve** the activity
- ▶ **Facilitate** report writing

WE ARE HUMANS — WARNING / 'EXPERT' DEBATE

- ▶ Human **interaction** with the constituency may be negatively impacted by a ticketing system
- ▶ Do not expose tickets to the constituency
- ▶ Automation is good... until it strips away the **social** aspects of our work

- ▶ Hunting for a solution started in early **2014**
- ▶ Solutions existed but **partially** fulfilled the requirements
- ▶ Office (*cough*), AbuseHelper, RTIR, MISP, CIF, Resilient Systems...
- ▶ Build vs. buy: given the requirements and our skills, we decided to **build**

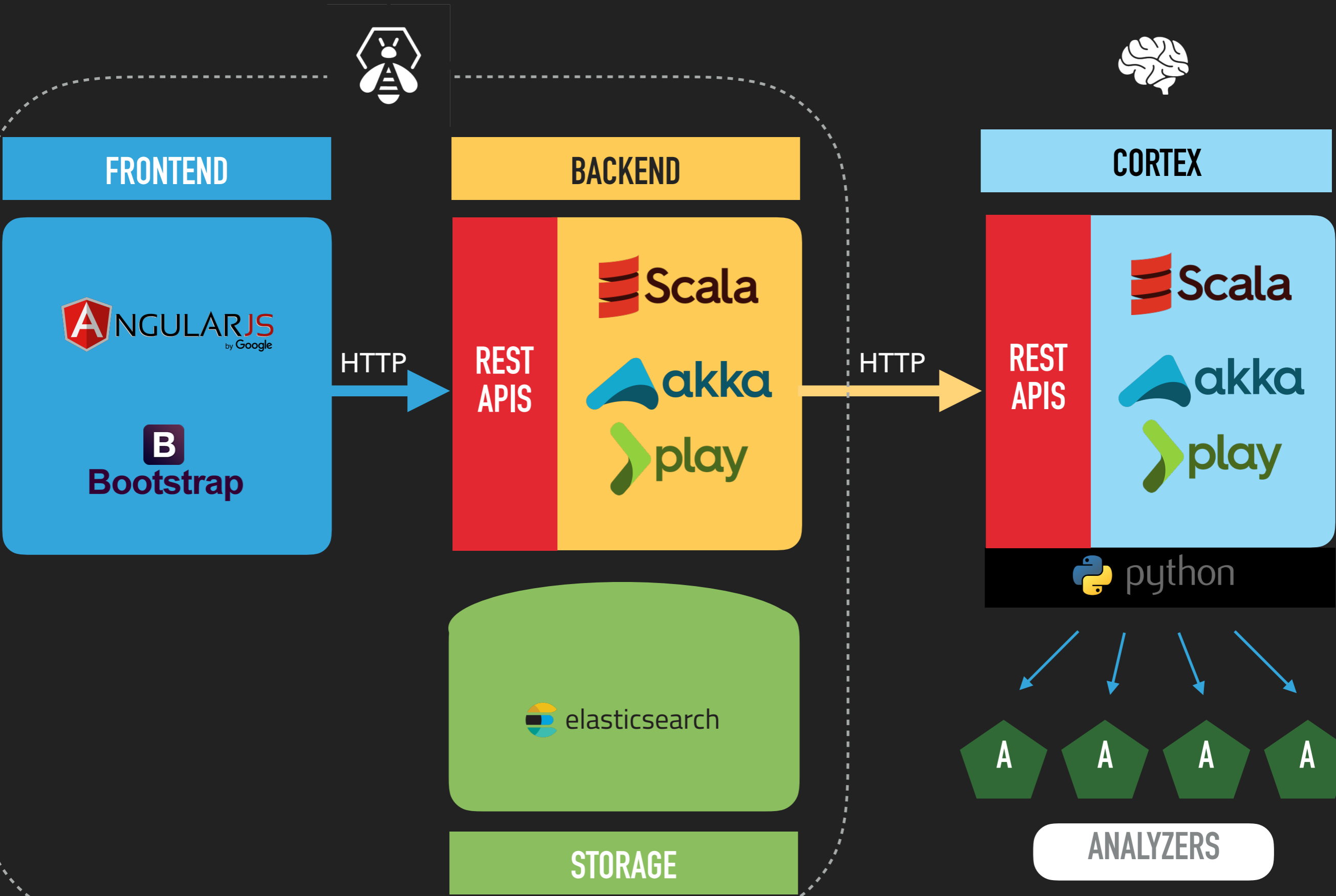


LEARNING FROM BEES

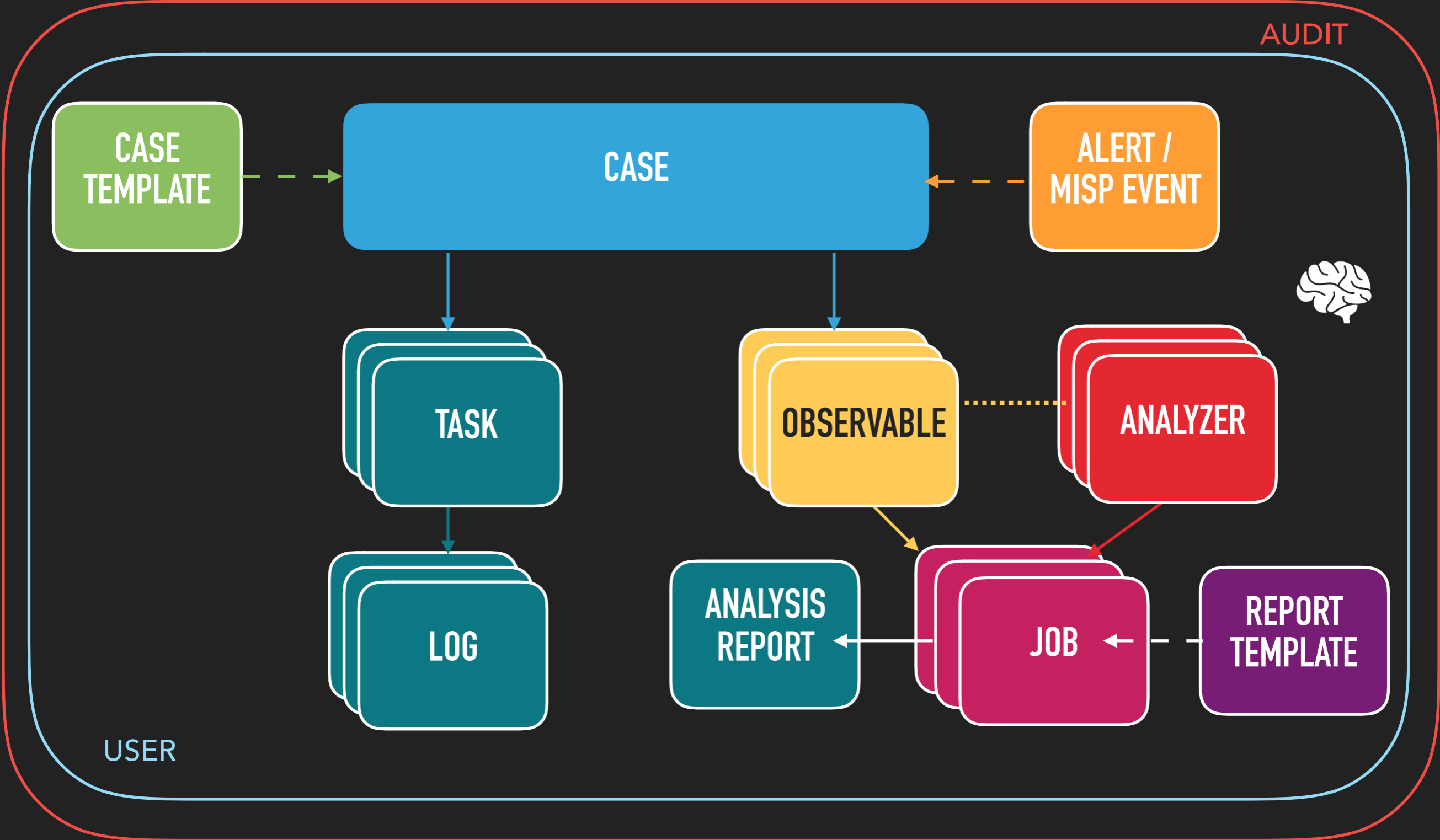
THEHIVE

- ▶ 3-IN-1
 - ▶ **Collaboration** platform
 - ▶ Task & work **log**
 - ▶ **Analysis** and storage platform
- ▶ Supports LDAP, Active Directory & local accounts for authentication
- ▶ Used by several CERTs/CSIRTs throughout the world

ARCHITECTURE



WORKFLOW



MAIN FEATURES

- ▶ **Import** & sync events from several **MISP** instances
- ▶ Preview **alerts** from multiple sources (SIEM, IDS, email...)
- ▶ **Handle** cases the way you want using **templates**
- ▶ **Analyze** observables through several **Cortex** instances
- ▶ Leverage **statistics** to **drive** the activity
- ▶ **Stay up-to-date** on new cases, tasks, analysis jobs thanks to the real-time **stream**

- ▶ **Automate** bulk observable **analysis** through a REST API
- ▶ Query analyzers through a **Web UI** to quickly **assess** the malicious nature of observables
- ▶ Analyzers can be developed in **any programming language** that is supported by Linux
- ▶ **Invoke MISP** expansion modules
- ▶ Can be **queried from MISP** to enrich events

23 ANALYZERS (AND MORE ARE COMING)

PASSIVETOTAL

FORTIGUARD URL
CATEGORY

HIPPOCAMPE

MAXMIND

SPLUNK SEARCH

CIRCL PSSL

CIRCL PDNS

GOOGLE SAFE
BROWSING

JOE SANDBOX

CUCKOO

MISP SEARCH

VIRUSTOTAL

DNSDB

VMRAY

MCAFFEE ATD

DOMAINTOOLS

ABUSE FINDER

YARA

FIREHOL

IRMA

FILEINFO

NESSUS

PHISHING
INITIATIVE

FAME

WHOISXMLAPI

OUTLOOK MSG
PARSER

OTXQUERY

PHISHTANK

INTELMQ

FIREEYE AX

HYBRID ANALYSIS

GET THE SOFTWARE

- ▶ TheHive and Cortex are available under an **AGPL** license
- ▶ Can be installed using **RPM, DEB, Docker** image, **binary** package or built from the **source** code
- ▶ Pre-requisites: Linux with JRE 8+, Chrome, Firefox, IE (11), and a decent computer
- ▶ <https://thehive-project.org/>



SHOW TIME

DEMO?

MAIN VIEW

List of cases (16 of 2320)

[+ Show live stream](#)

[Quick Filters ▾](#) [Sort by ▾](#)

[Stats](#) [Filters](#) 15 per page

1 filter(s) applied: **status: Open** [✕](#) [Clear filters](#)

[First](#) [Previous](#) **1** [2](#) [Next](#) [Last](#)

Title	Severity	Tasks	Observables	Assignee	Date
#2301 - [redacted] WannaCry malware_classification:malware-category="Ransomware" circl:incident-classification="vulnerability" misp-galaxy:ransomware="WannaCry" misp ioc src:INCIBE src:CIRCL_65 src:TRUESEC.be_9181 dnc:malware-type="Ransomware" enisa:nefarious-activity-abuse="ransomware" osint:source-type="technical-report" src:eCrimeLabs_3868 osint:source-type="blog-post" wannacrypt admiralty-scale:source-reliability="b" src:CERT-Bund Merged from Case #2300 and Case #2299	H	12 Tasks	1145	AB	05/15/17 9:11
#2280 - [redacted] #1700236 Anti Public Combo List src:l[redacted] :DATA_BREACH=Email addresses	H	2 Tasks	0		05/11/17 11:50
#2319 - #7155 New XData ransomware src:TRUESEC.be_9181 malware_classification:malware-category="Ransomware"	H	No Tasks	12		05/20/17 7:12

 Updated by System 🕒 a minute

 **#7156 OSINT - New SMB Worm Uses Seven NSA Hacking Tools. WannaCry Used Just Two**

artifacts: 0

tlp: 0

caseTemplate:

description: Imported from MISP Event #7156, created at Sun May 21 09:53:45 CEST 2017

tags: ["src:CIRCL_65"]

lastSyncDate: 1495354503000

status: Updated

severity: 3


title: #7156 OSINT - New SMB Worm Uses Seven NSA Hacking Tools. WannaCry Used Just Two

 Updated by  🕒 21 minutes

 **#7153 Trojan**

status: Ignored

 Updated by  🕒 21 minutes

 **#7152 Spam**

status: Ignored

 Added by  🕒 21 minutes

 **[MISP] #7154 HookAds Malvertising Campaign leads to RIG EK drops LatentBot and Ramnit**

This case contains 2 tasks [See all](#)

This case contains 72 observables [See all](#)

description: Imported from MISP Event #7154, created at Fri May 19 17:43:47 CEST 2017

 #2320 - [MISP] #7154 HookAds Malvertising Campaign leads to RIG EK drops LatentBot and Ramnit

CASE VIEW

M Case # 2317 - #7151 Malicious network activity (week 20/17) [+ Show live stream](#)

Created by Fri, May 19th, 2017 9:19 +02:00 [13 Related cases](#)

[Close](#) [Flag](#) [Merge](#)

[Summary](#) [Tasks **1**](#) [Observables **54**](#)

Basic information

Severity **M**

TLP **TLP-WHITE**

Title #7151 Malicious network activity (week 20/17)

Assignee

Date Fri, May 19th, 2017 9:19 +02:00

Tags **src-CERT-EU_8993**

Description

Imported from MISP Event #7151, created at Fri May 19 09:19:09 CEST 2017

Related cases

Newest (Case # 2313 - [MISP] #7140 Malspam 2017-05-17 Invoice)

Created on **2017-05-18**

Shares **2 observables**

Tagged as

Type:OSINT **misp** **ioc** **src-CIRCL_65**

Oldest (Case # 1730 - [MISP] #4979 Malicious network activity (week 45))

Created on **2016-11-15**

Shares **1 observable**

Tagged as

misp **ioc** **src-CERT-EU_8993**

[See all \(13 related cases\)](#)

Metrics

[+ Add metric ▾](#)

No metrics need to be set

CASE VIEW

Close Case #2319

 You are about to close Case #2319. Are you sure you want to continue?








Status *

Incident

True Positive False Positive Indeterminate Other

 There aren't enough elements to tell that there is something malicious (original message has been deleted and not transmitted, IOC lookup with 0 hits ...)

Summary *

B *I* **H** ~~S~~        [Preview](#)

Close summary

Cancel

* Required field

Close case


LOG VIEW


Summary Tasks 12 Observables 1145 Analyses, white-papers et 1


Analyses, white-papers et éléments techniques

📌 🗒️ + Add new task log ⬆ Sort by: Newest first ▾ 10 per page


Owner	[Redacted]
Date	Mon, May 15th, 2017 10:38 +02:00
Status	InProgress
Description	Not specified


 [Redacted] Wed, May 17th, 2017 14:27 +02:00 🗑️

 Un mémo technique synthétisant les résultats actuels des analyses de [Redacted] sur l'attaque et fournissant des marqueurs de compromission que vous pourrez utiliser pour faciliter la détection.




[Redacted]
technique_2017([Redacted]).docx

 [Redacted] Mon, May 15th, 2017 11:37 +02:00 🗑️

 Analyse/Rapport [Redacted]

[https://\[Redacted\]](https://[Redacted])



OBSERVABLE VIEW

Case # 2319 - #7155 New XData ransomware

[+ Show live stream](#)

Created by Sat, May 20th, 2017 7:12 +02:00

[Close](#) [Flag](#) [Merge](#)

[Summary](#) [Tasks 0](#) [Observables 12](#)

Action [+ Add observable\(s\)](#)

[Stats](#) [Filters](#) 15 per page

List of observables (12 of 12)

<input type="checkbox"/>	Type	Data/Filename	Analysis	Date added
<input type="checkbox"/>	mail	bil@thwonderfulday[.]com src:MISP-BDF ioc:misp MISP:type=email-dst MISP:category=Network activity	No reports available	05/20/17 7:12
<input type="checkbox"/>	mail	bob@thwonderfulday[.]com src:MISP-BDF ioc:misp MISP:type=email-dst MISP:category=Network activity	No reports available	05/20/17 7:12
<input type="checkbox"/>	mail	trevor@thwonderfulday[.]com src:MISP-BDF ioc:misp MISP:type=email-dst MISP:category=Network activity	No reports available	05/20/17 7:12
<input type="checkbox"/>	mail	bilbo@colocasia[.]org src:MISP-BDF ioc:misp MISP:type=email-dst MISP:category=Network activity	No reports available	05/20/17 7:12

OBSERVABLE VIEW

Observable Information

TLP	TLP:WHITE
Date added	Sat, May 20th, 2017 7:09 +02:00
Is IOC	☆
Labels	src: ioc:misp MISP:type=aha256 MISP:category=Artifacts dropped
Description	Not specified

Observable Links

Observable seen in 0 other case(s)

Observable Analyzers

Run all

Analyzer	Cortex Server	Last analysis	Action
VirusTotal_GetReport_2_0 VirusTotal get report: provides the last report of a file, hash, domain or ip	interne	None	
PassiveTotal_Ssl_Certificate_History_1_0 PassiveTotal Ssl Certificate History Lookup	interne	None	
MISP_Search_1_0 Search MISP event that have the observable provided as an input	externe	None	
OTXQuery_1_0 Query AlienVault OTX for IPs, Domains, URLs, or File Hashes	interne	None	
PassiveTotal_Ssl_Certificate_Details_1_0 PassiveTotal Ssl Certificate Details Lookup	interne	None	

OBSERVABLE VIEW

TheHive	+ New Case	My tasks 1	Waiting tasks 17	Alerts 0	Statistics	Case, user, URL, hash, IP, domain ...	Saâd Kadhi
PassiveTotal_Ssl_Certificate_History_1_0						interne	None
PassiveTotal Ssl Certificate History Lookup							
MISP_Search_1_0						externe	✓ Mon, May 22nd, 2017 14:14 +02:00
Search MISP event that have the observable provided as an input							
OTXQuery_1_0						interne	None
Query AlienVault OTX for IPs, Domains, URLs, or File Hashes							
PassiveTotal_Ssl_Certificate_Details_1_0						interne	None
PassiveTotal Ssl Certificate Details Lookup							

Report for MISP_Search_1_0 analysis of Mon, May 22nd, 2017 14:14 +02:00

Show Raw Report

Detailed Information

New XData ransomware

Event ID 7155

UUID 591fcf16-8d94-4cc6-98da-76d9ac130003

Publish Date Sat, May 20th, 2017 7:45 +02:00

Tags TLP:WHITE malware_classification:malware-category="Ransomware"

OBSERVABLE VIEW

Report for VirusTotal_GetReport_2_0 analysis of Mon, May 22nd, 2017 14:15 +02:00

[Show Raw Report](#)

Summary

Score 45/61

Last analysis date 2017-05-22 12:05:02

Virus Total [View Full Report](#)

Scans

Scanner	Detected	Result	Details	Update	Version
Bkav				20170522	1.3.0.8876
MicroWorld-eScan		Gen:Variant.Razy.175324		20170522	12.0.250.0
nProtect				20170522	2017-05-22.02
CMC				20170521	1.1.0.977
CAT-QuickHeal				20170522	14.00
McAfee		RDN/Generic.hra		20170522	6.0.6.653
Malwarebytes				20170522	2.1.1.1115
VIPRE		Trojan.Win32.Generic!BT		20170522	58266

OBSERVABLE VIEW

Summary

Tasks 0

Observables 12

d174f0c6ded55eb315320750a

[HASH]: d174f0c6ded55eb315320750aaa3152fc241acbfaef662bf691ffd0080327ab9

MISP: 1 record(s)

VT: 45/61 Scans(61)

Observable Information

TLP **TLP:WHITE**

Date added Sat, May 20th, 2017 7:09 +02:00

Is IOC ☆

Labels **src:1** **ioc:misp** **MISP:type=sha256** **MISP:category=Artifacts dropped**

Description *Not specified*

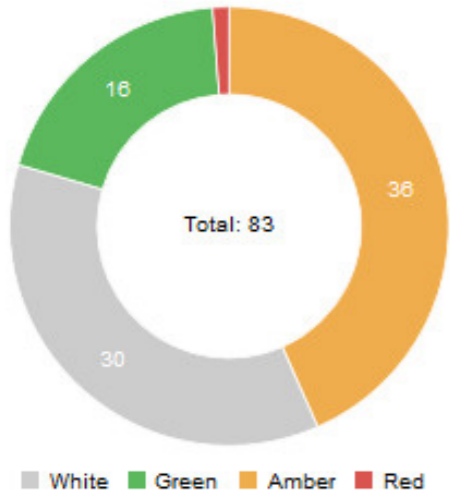
Observable Links

Observable seen in 0 other case(s)

STATISTICS

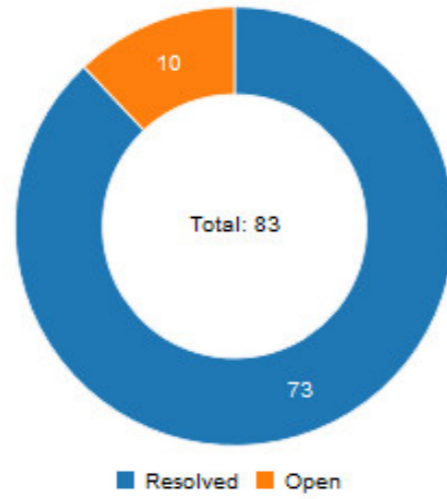
Cases by TLP

Save as image



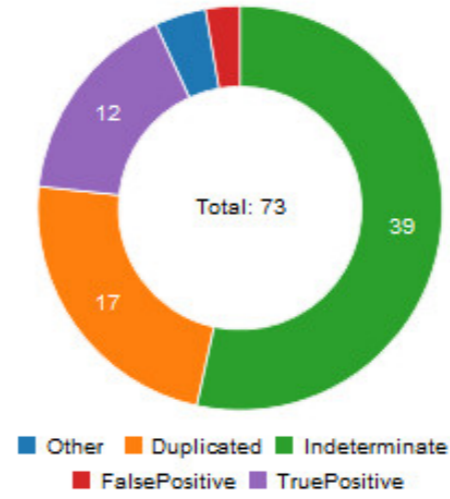
Cases by status

Save as image



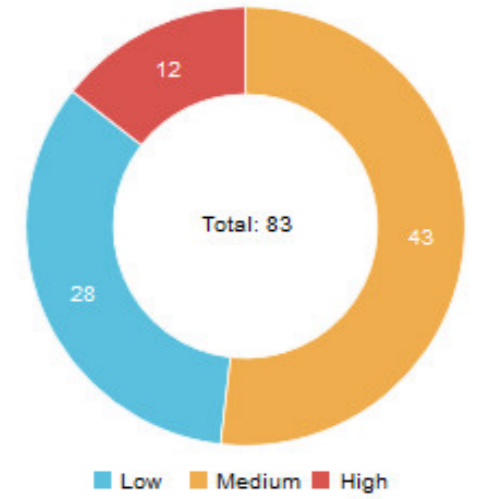
Resolved cases by resolution

Save as image



Cases by Severity

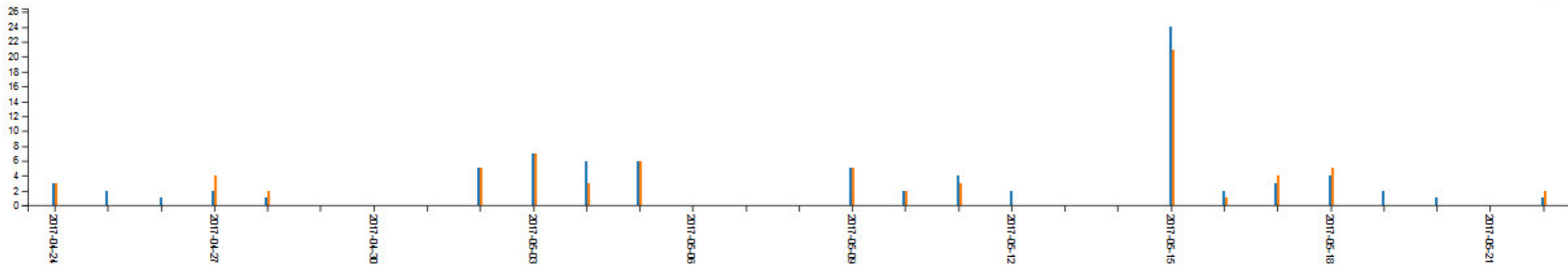
Save as image



Cases over time

Interval By day

Save as image

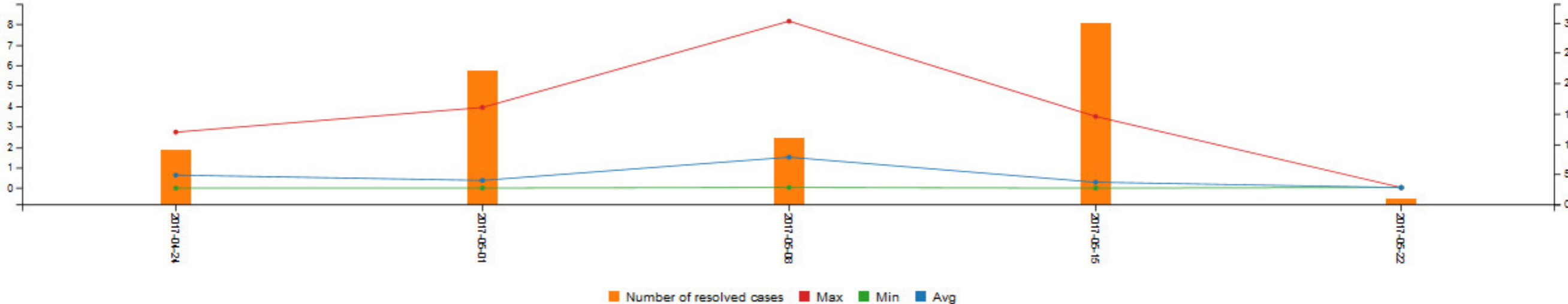


STATISTICS

Cases handling over time

Interval By week

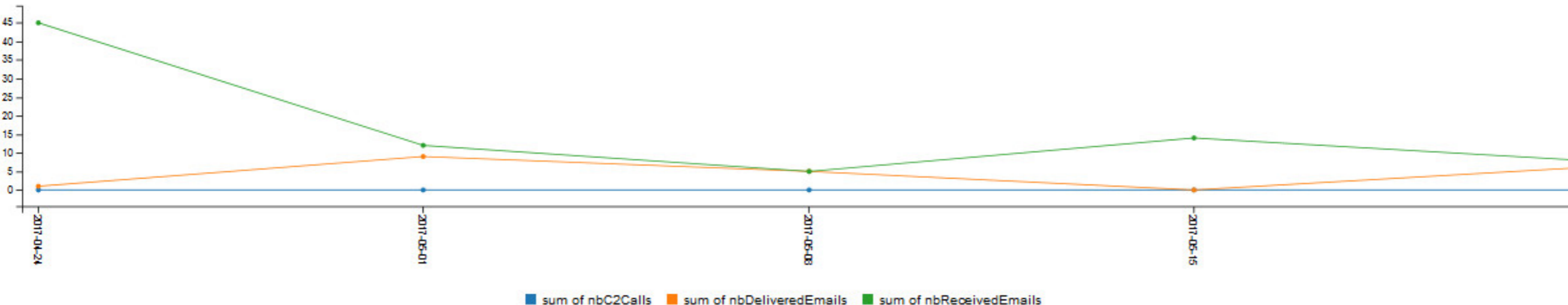
Save as image



Case metrics over time

Metrics 3 checked Aggregations 1 checked Interval By week

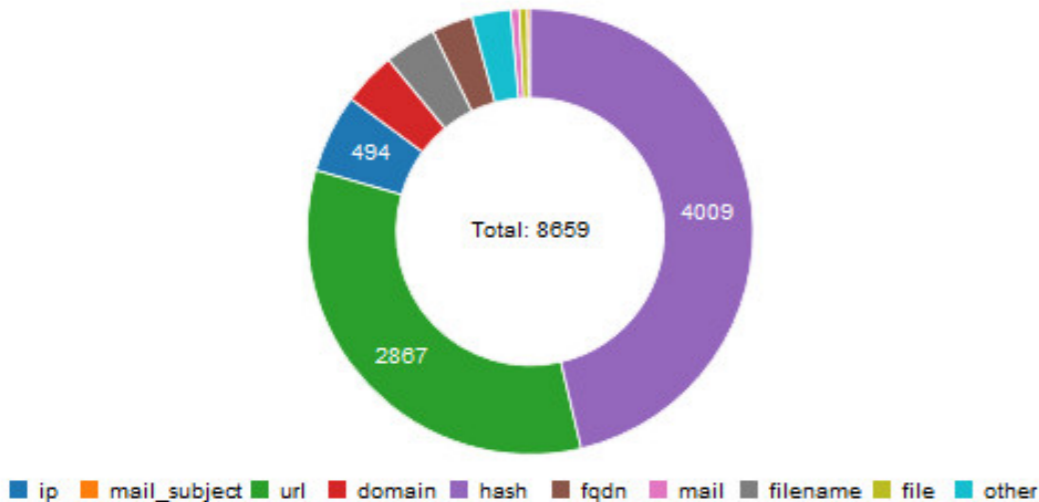
Save as image



STATISTICS

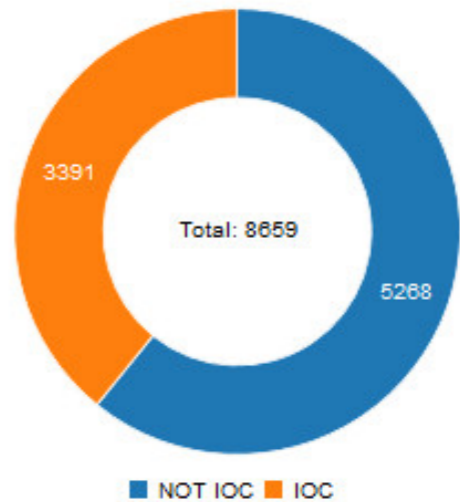
Observables by Type

Save as image



Observables by IOC flag

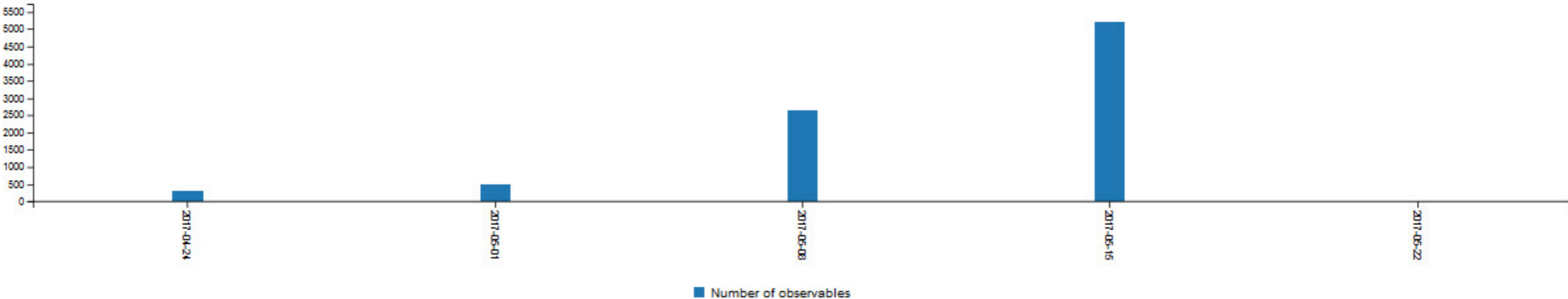
Save as image



Observables over time

Interval By week [dropdown] [search icon]

Save as image



Analyzers

Data types	
ip	21
domain	20
url	12
email	1
certificate_hash	1
hash	7
fqdn	11
mail	2
other	2
file	9
filename	1
mail_subject	1
regexp	1
registry	1
uri_path	1
user-agent	1

Abuse_Finder Version: 1.0 Author: CERT-BDF License: AGPL-V3 [▶ Run](#)

Use CERT-SG's Abuse Finder to find the abuse contact associated with domain names, URLs, IPs and email addresses

Applies to: [ip](#) [domain](#) [url](#) [email](#)

CIRCLPassiveDNS Version: 1.0 Author: Nils Kuhnert, CERT-Bund License: AGPL-V3 [▶ Run](#)

Check CIRCL's Passive DNS for a given domain or URL

Applies to: [domain](#) [url](#)

CIRCLPassiveSSL Version: 1.0 Author: Nils Kuhnert, CERT-Bund License: AGPL-V3 [▶ Run](#)

Check CIRCL's Passive SSL for a given IP address or a X509 certificate hash

Applies to: [ip](#) [certificate_hash](#) [hash](#)

DNSDB_DomainName Version: 1.1 Author: CERT-BDF License: AGPL-V3 [▶ Run](#)

Provide history records for a domain using DNSDB Passive DNS service

Applies to: [domain](#)

DNSDB_IPHistory Version: 1.0 Author: CERT-BDF License: AGPL-V3 [▶ Run](#)

Provide history records for an IP address using DNSDB Passive DNS service

Applies to: [ip](#)

Run new analysis

TLP AMBER

Data Type file

File Drop file or click

Analyzers

- File_Info_1_0
- JoeSandbox_File_Analysis_Inet_1_0
- JoeSandbox_File_Analysis_Noinet_1_0
- MISP_Search_1_0
- Msg_Parser_1_0
- OTXQuery_1_0
- Virusshare_1_0
- VirusTotal_GetReport_2_0
- VirusTotal_Scan_2_0
- Yara_1_0

Cancel Start

Applies to: ip

Job details

[← Back to list](#)

⚙️ VirusTotal_GetReport_2_0

Artifact

[HASH]

2e8dc58a36806e13cd61e4a25f38c9ee

Date

a minute ago

Status

Success

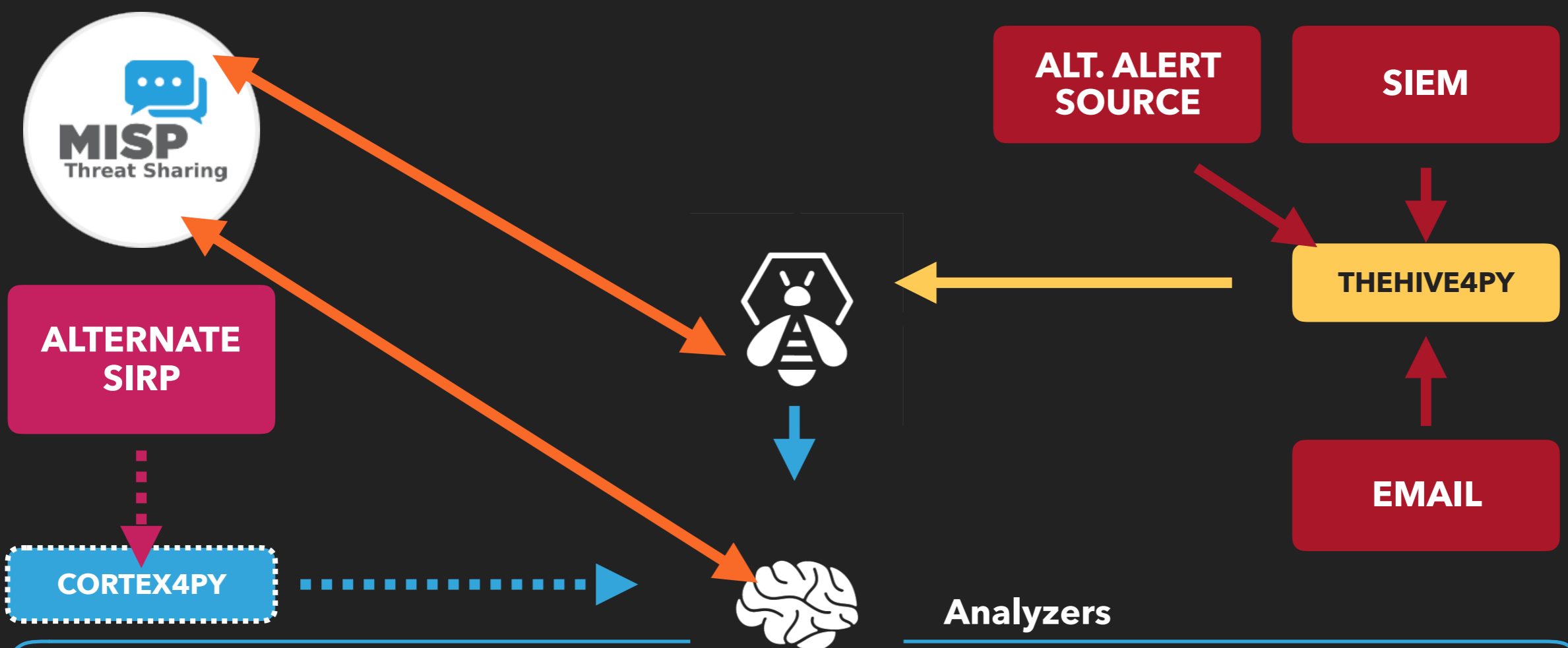
Job report

```
{
  "artifacts": [
    {
      "data": "aefe7efa7236c6ef63d4a970f3756de4d32049dc",
      "attributes": {
        "dataType": "hash"
      }
    },
    {
      "data": "2e8dc58a36806e13cd61e4a25f38c9ee",
      "attributes": {
        "dataType": "hash"
      }
    },
    {
      "data": "https://www.virustotal.com/file/8b3b8fba04773b40d9639ff57755c7f96d8359b23927d0f72654f81db671c67d",
      "attributes": {
        "dataType": "url"
      }
    },
    {
      "data": "8b3b8fba04773b40d9639ff57755c7f96d8359b23927d0f72654f81db671c67d",
      "attributes": {
        "dataType": "hash"
      }
    },
    {
      "data": "2e8dc58a36806e13cd61e4a25f38c9ee",
      "attributes": {
        "dataType": "hash"
      }
    },
    {
      "data": "1.3.0.8876",
      "attributes": {
        "dataType": "ip"
      }
    }
  ],
}
```




COME AGAIN?

THE BIG PICTURE



Analyzers

ABUSE FINDER	VIRUSTOTAL	PASSIVETOTAL	MAXMIND
HIPPOCAMPE	PHISHTANK	OTXQUERY	PHISHING INITIATIVE
DOMAINTOOLS	URLCATEGORY	DNSDB	FILEINFO
OUTLOOK MSGPARSER	MISP	NESSUS	JOE SANDBOX
VMRAY	CIRCL PSSL	CIRCL PDNS	YARA
GOOGLE SAFE BR.	VMRAY	URLQUERY	WHOISXMLAPI

THANK YOU!

THEHIVE PROJECT

CORE TEAM

THOMAS FRANCO

SAÂD KADHI

JÉRÔME LEONARD

MAIN CONTRIBUTORS

NABIL ADOUANI

CERT-BDF

CONTRIBUTORS

CERT-BUND

RÉMI POINTEL

ERIC CAPUANO

MEHDI ASCHY

ANTOINE BRODIN

GUILLAUME
ROUSSE