50TH TF-CSIRT MEETING AND FIRST REGIONAL SYMPOSIUM FOR EUROPE

TLP:GREEN

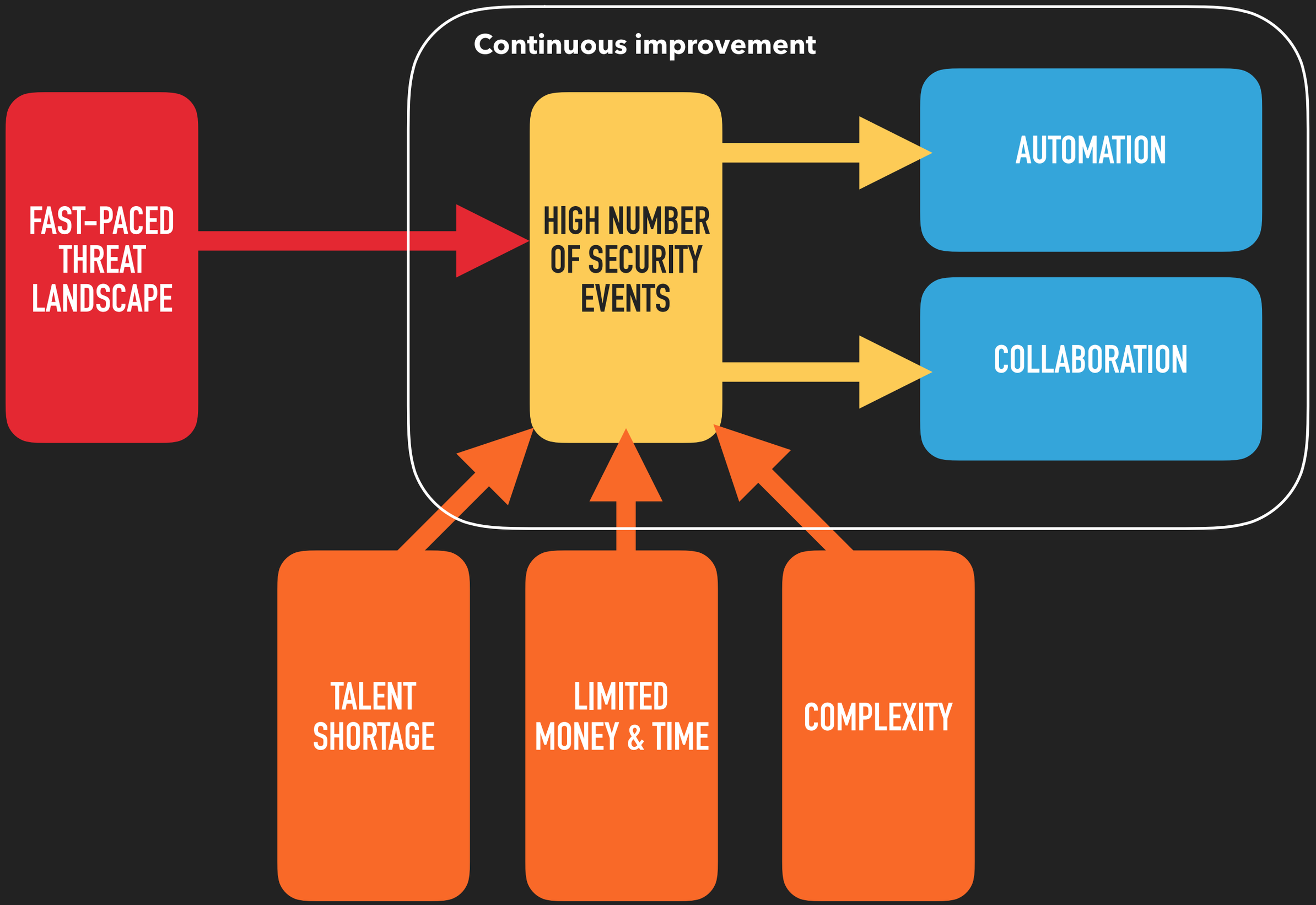
A SCALABLE, OPEN SOURCE AND FREE INCIDENT PLATFORM

Saâd Kadhi
TheHive Project

THREATS & REACTION

FINDINGS

DRIVING DOWN THE TIME TO REACT



WORK AS A TEAM

- DFIR is a team work
- FOSS mantra: 'with enough eyeballs, all bugs are shallow'
- DFIR mantra: 'with enough eyeballs, skills and mindsets, all threats are shallow'

SHARING IS CARING

- And here we are, tired but happy
- The case has been investigated, IOCs found and proper response done
- Wouldn’t they be useful to peers to defend themselves?
- And they will come up hopefully with complementary IOCs that were unbeknownst to us

OPSEC ISSUES

- All observables are not created equal
- Their TLP, among other attributes, may vary
- A single case may involve observables from multiple sources
- TLP drive analysis and sharing
- Ex. a TLP:AMBER file must not be submitted to VT
- But its hash may be

KEEP MANAGEMENT HAPPY

- Since donuts & pie charts are ~~eye candy~~ essential management tools…
- Operational, meaningful statistics should be produced
- To drive the DFIR activity and continuously improve it

SEEKING SOLUTIONS

SPECS

AUTOMATION & COLLABORATION

- Let many analysts work on multiple cases, sometimes simultaneously
- Store observables, mark some as IOCs, make their analysis as simple as possible
- Index observables, cases and any noteworthy evidence or reference
- Let analysts search through them

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 or SIEM alerts
- Generate statistics to drive and improve the activity
- Facilitate report writing

WE ARE HUMANS

- 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

WHAT'S ON THE MARKET

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

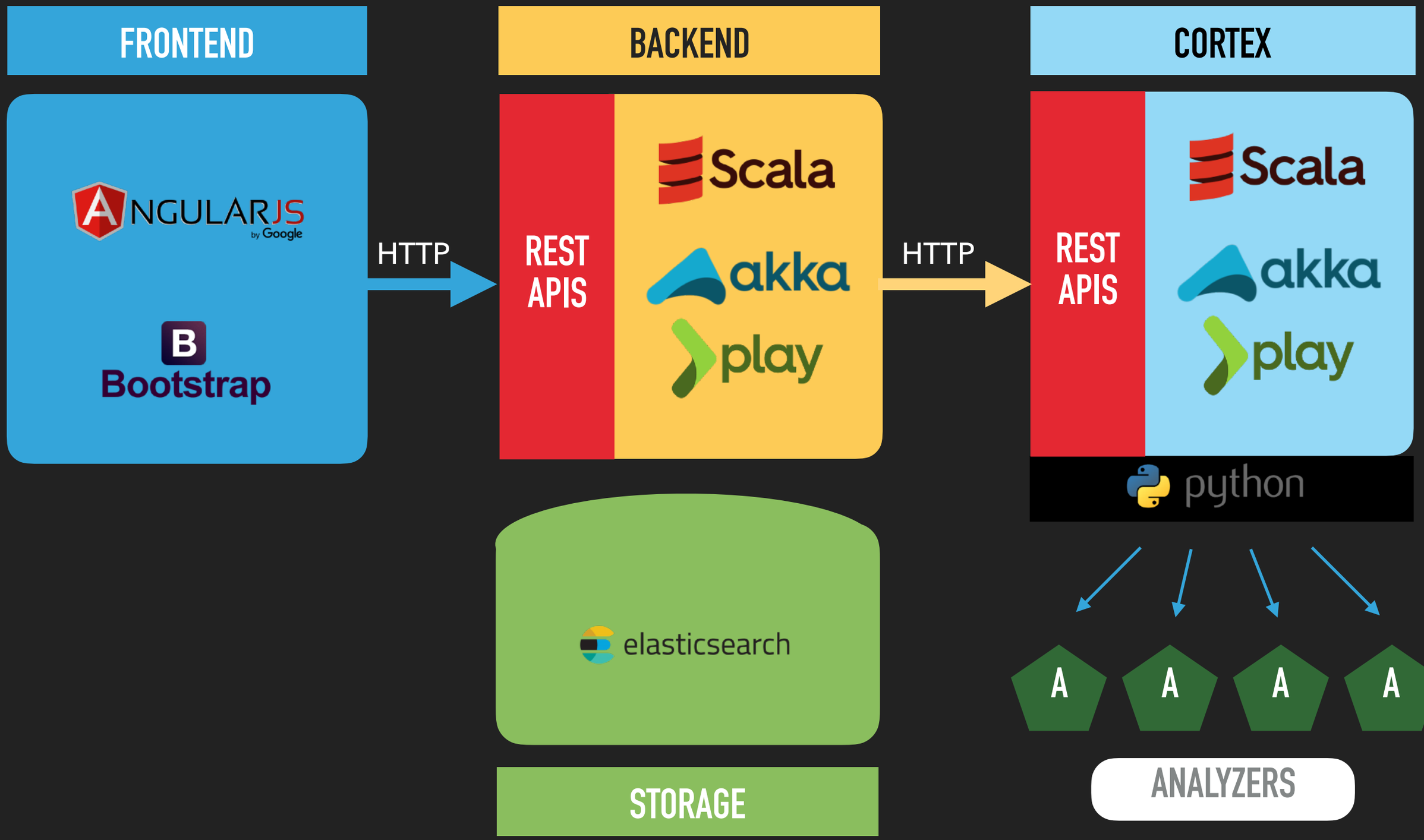
LEARNING FROM BEES

THEHIVE

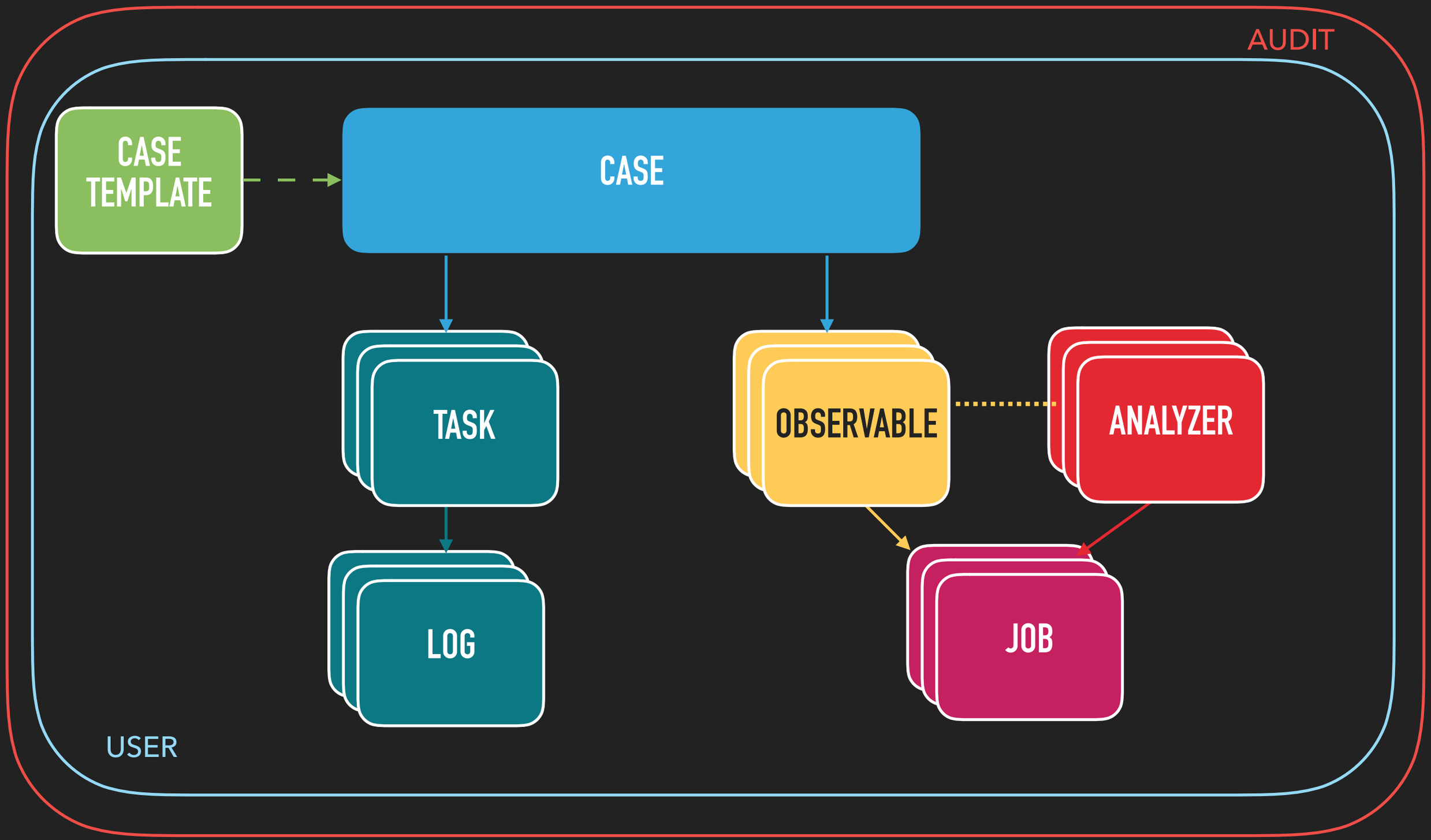
TheHive

- 3-IN-1
  - Collaboration platform
    - Task & work log
    - Analysis and storage platform
- Used by a CERT team of 12 analysts on a daily basis since Oct 2014
- LDAP & Active Directory support for authentication

ARCHITECTURE



WORKFLOW


AUDIT
CASE TEMPLATE
CASE
TASK
LOG
OBSERVABLE
ANALYZER
JOB
USER

USE CASES (EXAMPLES)

- Have we already seen these observables somewhere else?
- Have we already handled a similar case in the past? What was the outcome?
- Is there something we do on a regular basis that we can automate?
- We have a set of heterogenous observables that we need to analyze

MAIN FEATURES

- Import and synchronize events from several MISP instances
- Analyze observables through one or several Cortex instances
- Leverage powerful statistics to drive the activity
- Stay up-to-date and get information about new cases, tasks, … thanks to the flow
- Handle cases the way you want using templates

CORTEX - STANDALONE ANALYSIS ENGINE

- 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

11 ANALYZERS

FILEINFO

OUTLOOK MSG PARSER

VIRUSTOTAL

JOE SANDBOX

DOMAINTOOLS

DNSDB

PASSIVE TOTAL

SPLUNK

FORTIGUARD URL CATEGORY

OTXQUERY

PHISHING INITIATIVE

PHISHTANK

HIPPOCAMPE

MAXMIND

MISP

SCALA-BILITY

- TheHive and Cortex are horizontally scalable
- Add more Elastic nodes and let them dance together
- Their REST APIs are stateless
- Add more back-ends / Cortex instances if there are load issues
- Currently missing: shared flow among back-ends through Apache kafka

PRE-REQUISITES

- Linux with JRE 8+
- Chrome, Firefox, IE (11)
- A decent computer

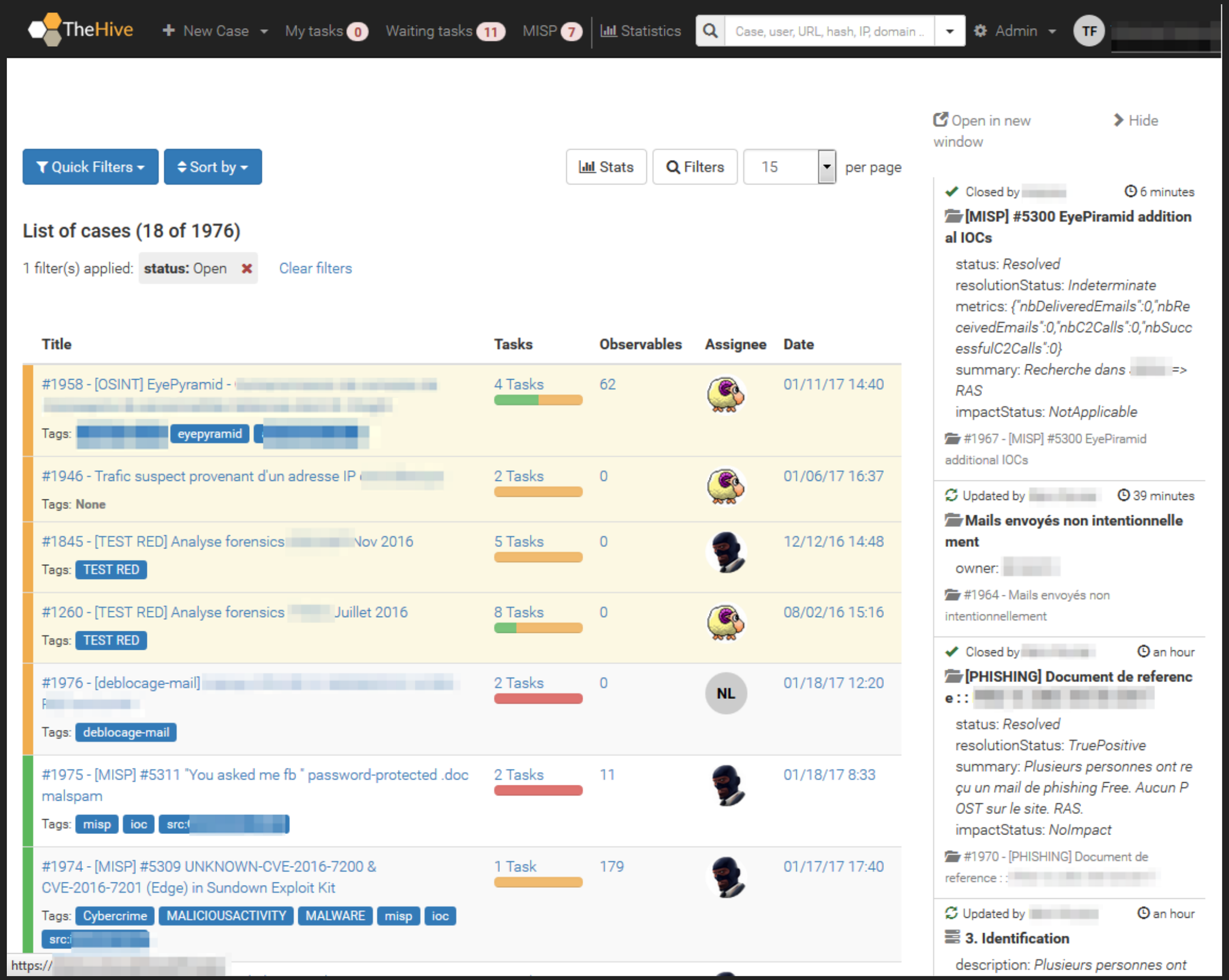
GET THE SOFTWARE

- TheHive is available under an AGPL license
- Source code hosted on GitHub by CERT-BDF
- Available as binary packages and Docker images
- Buckfast (2.10) and Cortex release scheduled for 3rd week of January

SHOW TIME

DEMO?

MAIN VIEW


TheHive
+ New Case
My tasks 0
Waiting tasks 11
MISP 7
Statistics
Case, user, URL, hash, IP, domain ..
Admin
TF
Quick Filters
Sort by
Stats
Filters
15
per page
List of cases (18 of 1976)
1 filter(s) applied: status: Open
Clear filters
Title
Tasks
Observables
Assignee
Date
#1958 - [OSINT] EyePyramid -
4 Tasks
62
01/11/17 14:40
Tags: eyepyramid
#1946 - Trafic suspect provenant d'un adresse IP
2 Tasks
0
01/06/17 16:37
Tags: None
#1845 - [TEST RED] Analyse forensics Nov 2016
5 Tasks
0
12/12/16 14:48
Tags: TEST RED
#1260 - [TEST RED] Analyse forensics Juillet 2016
8 Tasks
0
08/02/16 15:16
Tags: TEST RED
#1976 - [deblocage-mail]
2 Tasks
0
NL
01/18/17 12:20
Tags: deblocage-mail
#1975 - [MISP] #5311 "You asked me fb " password-protected .doc malspam
2 Tasks
11
01/18/17 8:33
Tags: misp ioc
#1974 - [MISP] #5309 UNKNOWN-CVE-2016-7200 & CVE-2016-7201 (Edge) in Sundown Exploit Kit
1 Task
179
01/17/17 17:40
Tags: Cybercrime MALICIOUSACTIVITY MALWARE misp ioc
Open in new window
Hide
Closed by
6 minutes
[MISP] #5300 EyePiramid additional IOCs
status: Resolved
resolutionStatus: Indeterminate
metrics: {"nbDeliveredEmails":0,"nbReceivedEmails":0,"nbC2Calls":0,"nbSuccessfulC2Calls":0}
summary: Recherche dans => RAS
impactStatus: NotApplicable
#1967 - [MISP] #5300 EyePiramid additional IOCs
Updated by
39 minutes
Mails envoyés non intentionnellement
owner:
#1964 - Mails envoyés non intentionnellement
Closed by
an hour
[PHISHING] Document de reference : :
status: Resolved
resolutionStatus: TruePositive
summary: Plusieurs personnes ont reçu un mail de phishing Free. Aucun POST sur le site. RAS.
impactStatus: NoImpact
#1970 - [PHISHING] Document de reference : :
Updated by
an hour
3. Identification
description: Plusieurs personnes ont
https://

THE FLOW

TheHive LIVE

Updated by [redacted] 30 minutes

[redacted]

Mr [redacted] a transféré le mail qu'il a reçu (cf [redacted]) à [redacted] Dans Splunk, (cf task identification) on voit des connexions de [redacted] sur l'url ``` [redacted] newslettertool2.1und1.de NOT user=- user=[redacted] ```

case1643_chargement_image_suite_transfert.csv

#1643 - [MALSPAM] Chronopost transfert de mail vu comme connexion

Added by [redacted] 32 minutes

[redacted]

Tracking Splunk depuis début de la semaine ``` index=[redacted] newslettertool2.1und1.de NOT user=- | table user | uniq 484 événements (01/10/16 00:00:00,000 à 21/10/16 12:05:13,000) ```

1643_newslettertool2_1und1_de(1).csv

#1643 - [MALSPAM] Chronopost 3. Identification

Added by [redacted] 35 minutes

[redacted]

Tracking [redacted] Generated: 21 Oct 2016 11:22 (GMT +02:00) Subject contains : suivi de l'envoi Période : 16/10/16 0h00 to 21 Oct 2016 11:19 (GMT +02:00)

CASE VIEW

TheHive | My tasks 0 | Waiting tasks 8 | Current | Closed | + New | MISP 0 | Case, user, URL, hash, IP, dor | Admin

Case # 1638 - [MISP] #4832 "Barclays Foreign Transaction (SWIFT)" LuminosityLink RAT malspam

Thu, Oct 20th, 2016 10:04 +02:00 (Closed at Thu, Oct 20th, 2016 14:08 +02:00 as **Indeterminate**) **19 Related cases**

Summary | Tasks 2 | Observables 10

Basic information

Severity	L
TLP	TLP:GREEN
Title	[MISP] #4832 "Barclays Foreign Transaction (SWIFT)" LuminosityLink RAT malspam
Date	Thu, Oct 20th, 2016 10:04 +02:00
Close date	Thu, Oct 20th, 2016 14:08 +02:00
Resolution Status	Indeterminate
Summary	Tracking sous => RAS tracking sous => RAS
Tags	misp ioc src: 6403
Description	Imported from MISP Event #4832, created at Thu Oct 20 02:30:48 CEST 2016 Links attributes : • https://www.virustotal.com/en/file/7f8158c8b683790322aaee9afe2694d3315585b049f05d1/analysis/1476866015/ • https://www.hybrid-analysis.com/sample/7f8158c8b683790322aaee9afe2694d3315585b049f05d1

Related cases

Newest (Case # 1640 - [MISP] #4828 Malspam with Reserve Bank of Australia lure)

Created on **2016-10-20**
Shares **1 observable**
Tagged as misp ioc src: 6403

Oldest (Case # 1193 - [MISP] #4078 "Bid" infostealer malspam)

Created on **2016-07-12**
Shares **1 observable**
Tagged as misp ioc src: 6403

See all (19 related cases)

Metrics

+ Add metric

Number of unique and successful C2 calls	0
Number of received emails	0
Number of unique C2 calls	0
Number of delivered emails	0

Closed by a day
[MISP] #4832 "Barclays Foreign Transaction (SWIFT)" LuminosityLink RAT malspam
status: *Resolved*
resolutionStatus: *Indeterminate*
metrics: *{"nbDeliveredEmails":0,"nbReceivedEmails":0,"nbC2Calls":0,"nbSuccessfulC2Calls":0}*
summary: *Tracking sous => RAS tracking sous => RAS*
impactStatus: *NotApplicable*
endDate: *Thu, Oct 20th, 2016 14:08 +02:00*
#1638 - [MISP] #4832 "Barclays Foreign Transaction (SWIFT)" LuminosityLink RAT malspam

Added by a day
Arnaud
Tracking sur les FQDN sous `````` l830977@varan:~$ search_es.py -f test -i logs-serai-201* --field FQDN -t 1000 --show {'sort': [{'Date': {'order': 'desc', 'ignore_unmapped': True}}], 'query': {'filtered': {'filter': {'terms': {'FQDN': [[mopol.m ...
#1638 - [MISP] #4832 "Barclays Foreign Transaction (SWIFT)" LuminosityLink RAT malspam Tracking SERAI

Completed by a day
Tracking
status: *Completed*
endDate: *Thu, Oct 20th, 2016 14:05 +02:00*
flag: *false*
#1638 - [MISP] #4832 "Barclays Foreign Transaction (SWIFT)" LuminosityLink RAT malspam Tracking SERAI

Added by a day

CASE VIEW

Close Case #1642

You are about to close Case #1642. Are you sure you want to continue ?

Incident

Status ✱ — True Positive | False Positive | **Indeterminate** | Other

There is not enough elements to tell that there is something malicious (original message has been delete and not transmitted, IOC lookup with 0 hit ...)

Summary ✱ — Tracking [redacted]: 0 HIT. Tracking [redacted]: 0 HIT. RAS.

Number of unique and successful C2 calls ✱ — 0

Number of received emails ✱ — 0

Number of unique C2 calls ✱ — 0

Number of delivered emails ✱ — 0

Cancel ✱ Required field Close case

LOG VIEW

M **Case # 1590 - Faux compte https://www.facebook.com/fr**

Sat, Oct 8th, 2016 16:00 +02:00 (Closed at Mon, Oct 10th, 2016 9:25 +02:00 as **True Positive**)

Summary | Tasks 3 | Observables 2 | **Eradication** | **Vérification** | **Détection**

Eradication

+ Add new task log

Owner

Date Mon, Oct 10th, 2016 9:23 +02:00

Close date Mon, Oct 10th, 2016 9:25 +02:00

Description

Compte signalé à puis fermé par Facebook.

Mon, Oct 10th, 2016 9:24 +02:00

Facebook nous informe que le compte a été fermé :

```
We removed the profile you reported

Oct 8

We reviewed the profile you reported for pretending to be someone they
're not. Since it violated our Community Standards, we removed it. Tha
nks for your report. We let                                know that the
ir profile has been removed, but not who reported it.
```

Mon, Oct 10th, 2016 9:23 +02:00

Le faux compte a été signalé à Facebook en suivant la procédure habituelle depuis le compte Facebook du CERT-BDF.

+ Added by 11 days

url: hxxps://www[.]facebook[.]com/profile[.]php?id=11

2 other observables have also been added See all

description: Faux compte FVdG

#1590 - Faux compte https://www.facebook.com /fr https://www.facebook.com /profile.php?id=11

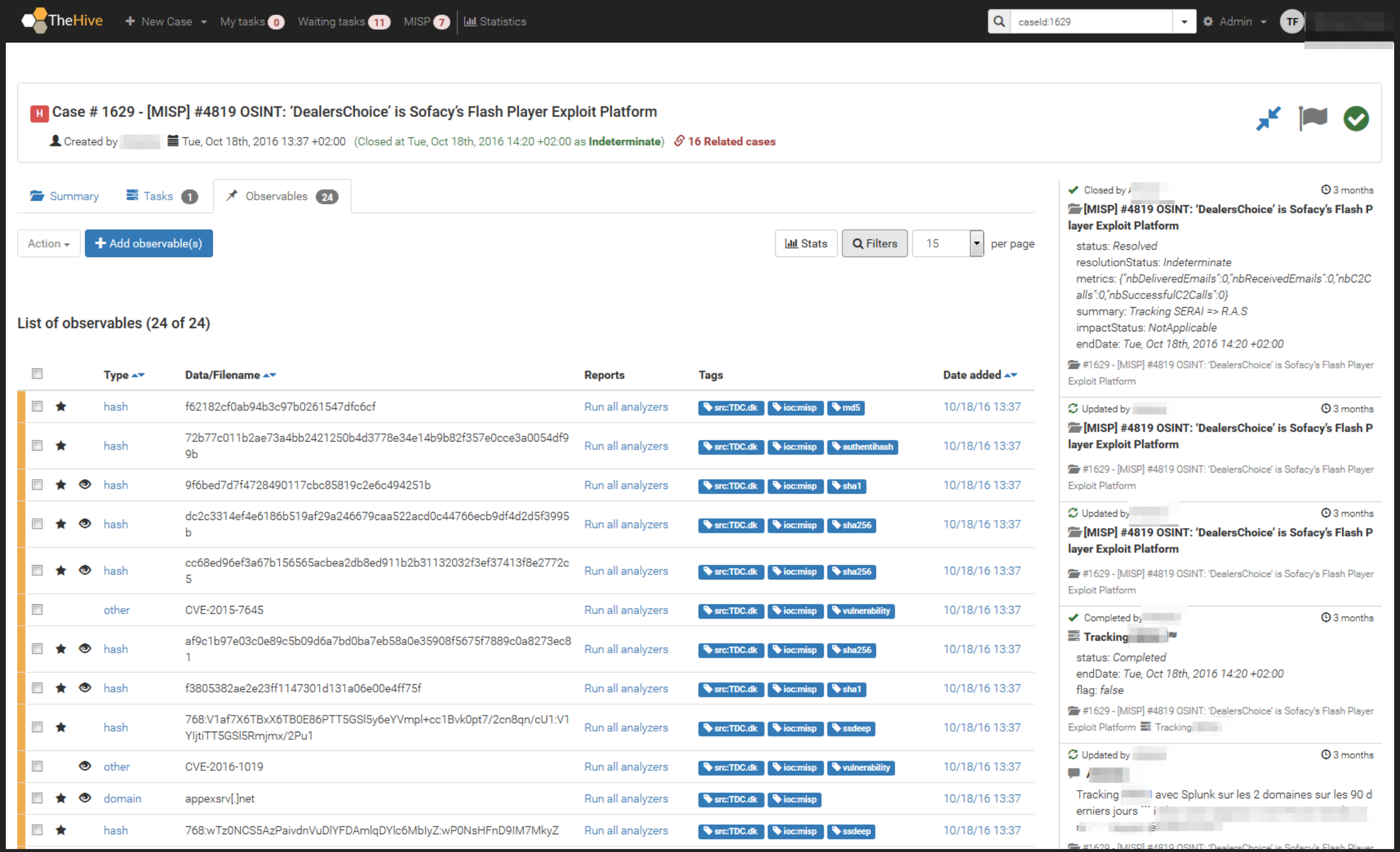
Closed by 11 days

Faux compte https://www.facebook.com/fr

status: *Resolved*
resolutionStatus: *TruePositive*
summary: *Le faux compte détecté et signalé le 7 octobre 2016 a été fermé par Facebook le 8 octobre 2016.*
impactStatus: *NoImpact*
endDate: *Mon, Oct 10th, 2016 9:25 +02:00*

#1590 - Faux compte https://www.facebook.com /fr

OBSERVABLE VIEW



M Case # 432 - doslegacy/ZAccess.QQA détecté

Created by [redacted] Wed, Nov 4th, 2015 14:16 +01:00 (Closed at Wed, Nov 4th, 2015 15:45 +01:00 as **True Positive**)

Summary | Tasks 3 | Observables 25 | **1234057937[.]exe[.]dr**

[FILE]: *1234057937.exe.dr*

VT: 26/53 Scans(53)

1234057937.exe.dr

Zip are protected with password "malware"

Observable Information

TLP	TLP:AMBER
Hash	**SHA256:** 47d86d19df67d1e5f96a1f5efd5884ca6acee06ba9020bf3d9b1878ed0f9c086 **SHA1:** b97fd6ff94546687b3c200916908c2978ad85680 **MD5:** 60b94649e20196e6893072000dcace0d
Date added	Wed, Nov 4th, 2015 15:19 +01:00
Is IOC	☆
Labels	PE
Description	Exe présent dans `Your personal_WT.zip`

Observable Links

Observable seen in 0 other case(s)

Observable Analyzers

Run all

Analyzer	Last analysis	Action
VirusTotal_GetReport_2_0 VirusTotal get report: provides the last report of a file, hash, domain or ip	✔ Wed, Jan 18th, 2017 16:15 +01:00	
VirusTotal_Scan_2_0		

OBSERVABLE VIEW

VirusTotal_GetReport_2_0 : VirusTotal get report: provides the last report of a file, hash, domain or ip Fri, Oct 21st, 2016 13:12 +02:00

Olevba analysis report. Submit a Microsoft Office File.

Report

Summary

Score 26/53

Last analysis date 2015-11-06 10:06:08

Scans

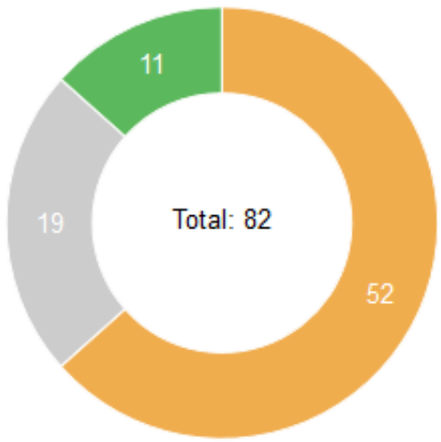
Scanner	Detected	Result	Details	Update	Version
Bkav				20151105	1.3.0.7383
MicroWorld-eScan		Gen:Variant.Kazy.763863		20151106	12.0.250.0
nProtect				20151106	2015-11-06.01
CMC				20151102	1.1.0.977
CAT-QuickHeal				20151106	14.00
McAfee		Downloader-FAHF!60B94649E201		20151106	6.0.6.653
Malwarebytes				20151106	2.1.1.1115
VIPRE		Trojan.Win32.Generic!BT		20151106	45042

STATISTICS

From 19-12-2016 To 18-01-2017 Tags Add tags

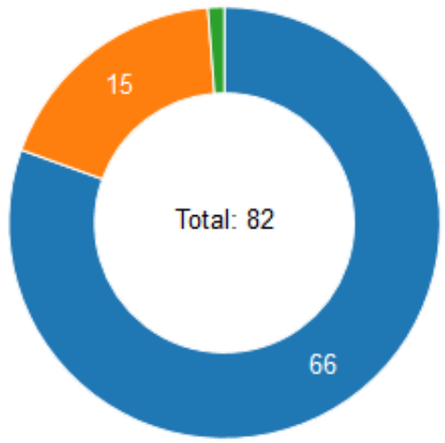
Cases by TLP

Save as image



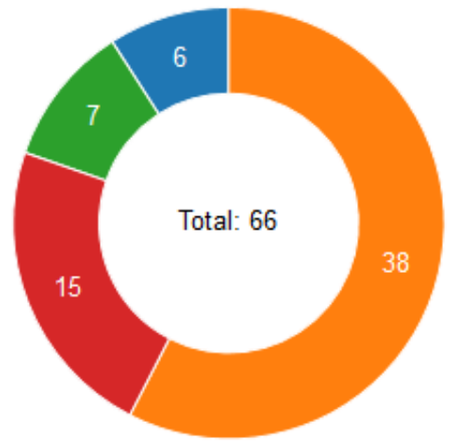
Cases by status

Save as image



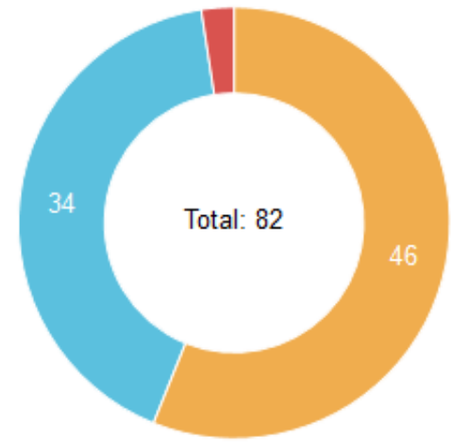
Resolved cases by resolution

Save as image



Cases by Severity

Save as image



Cases over time

Interval By month

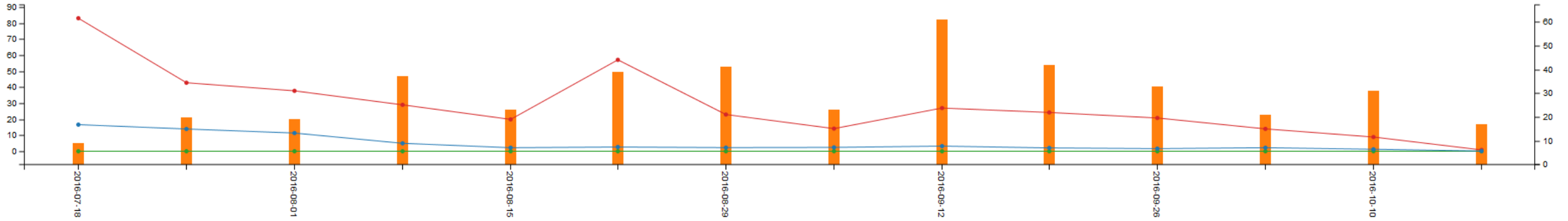
Save as image

STATISTICS

Cases handling over time

Interval By week

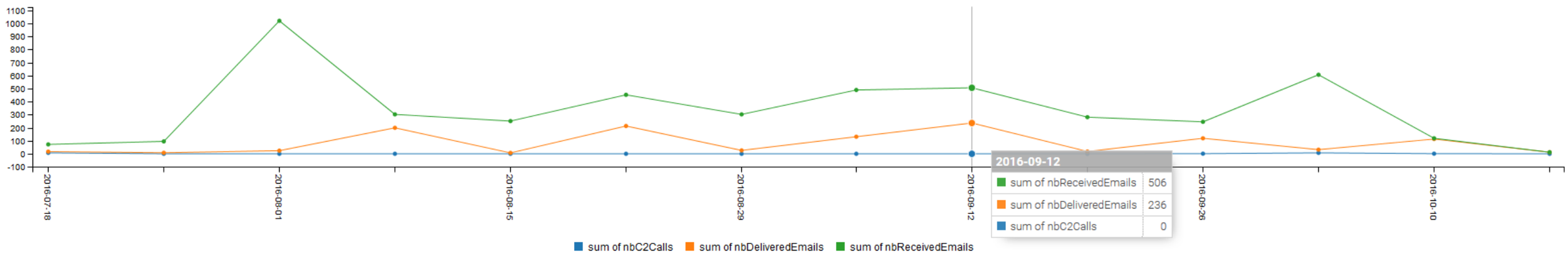
Save as image



Case metrics over time

Metrics 3 checked **Aggregations** 1 checked **Interval** By week

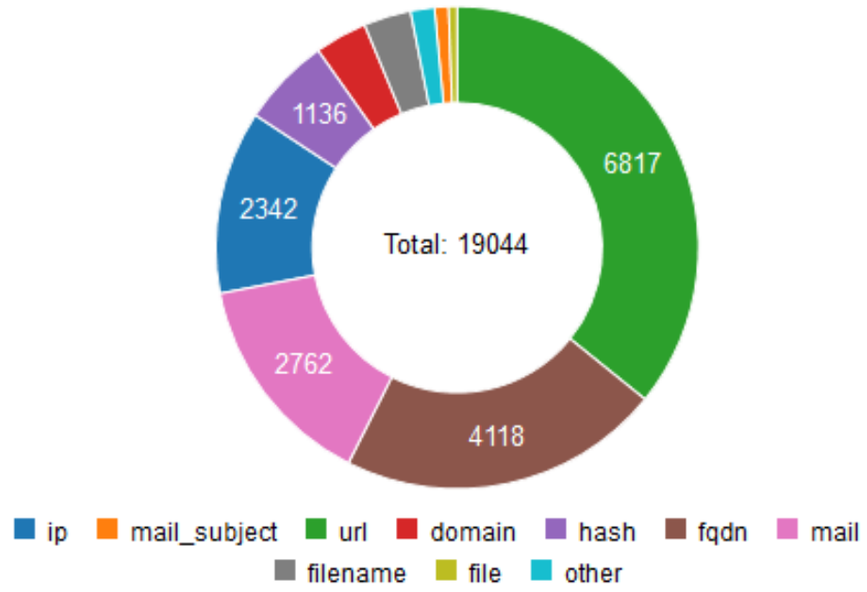
Save as image



STATISTICS

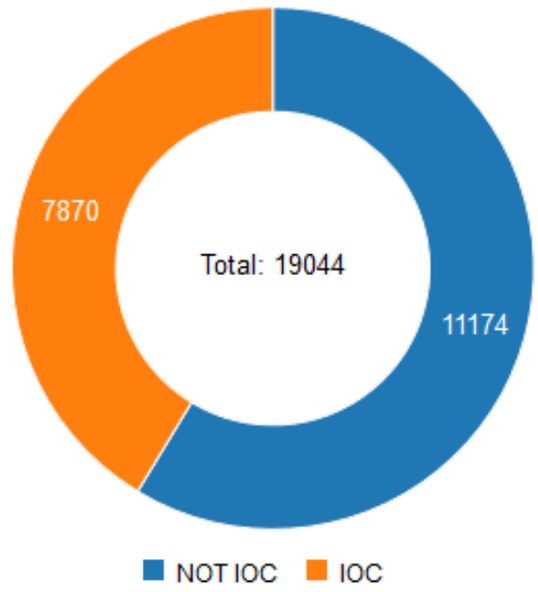
Observables by Type

Save as image



Observables by IOC flag

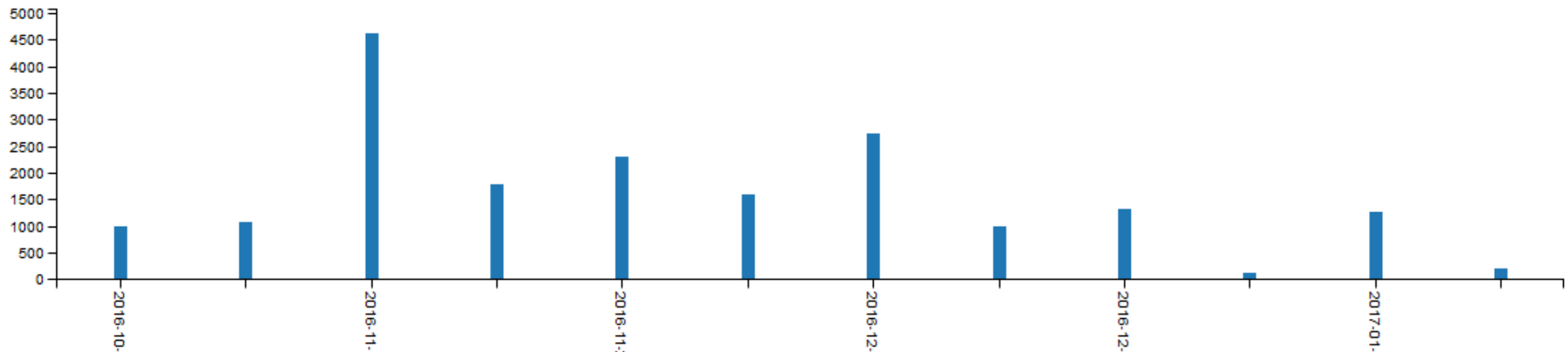
Save as image



Observables over time

Interval: By week

Save as image



CORTEX

Cortex | + New Analysis | Analyzers | Jobs

Analyzers

Data types

- ip 9
- domain 10
- fqdn 3
- file 5
- url 7
- mail 1
- other 1
- hash 2

Search for analyzer description

DNSDB_IPHistory (Version: 1.0) ▶ Run

DNSDB Passive DNS query for IP history : Provides history records for an IP

Applies to: ip

DNSDB_DomainName (Version: 1.1) ▶ Run

DNSDB Passive DNS query for Domain Names : Provides history records for a domain

Applies to: domain

DNSDB_NameHistory (Version: 1.0) ▶ Run

DNSDB Passive DNS query for domain/host name history : Provides history records for an domain/host

Applies to: fqdn

Msg_Parser (Version: 1.0) ▶ Run

Outlook .msg file parser

Applies to: file

Fortiguard_URLCategory (Version: 1.0) ▶ Run

URL Category by Fortiguard: checks the category of a specific URL or domain

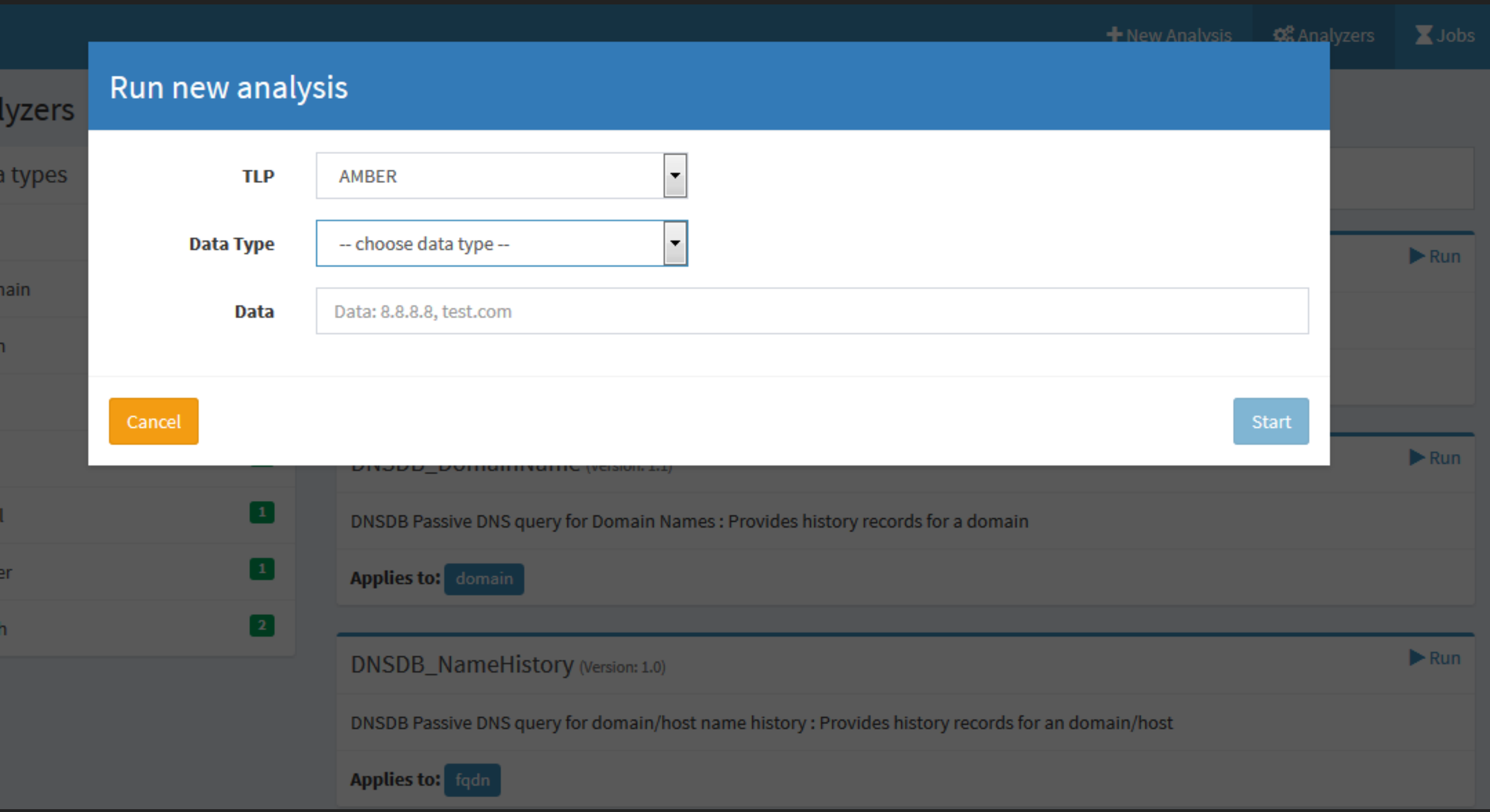
Applies to: domain url

File_Info (Version: 1.0) ▶ Run

Technical information about a File.

Applies to: file

CORTEX


New Analysis
Analyzers
Jobs
Run new analysis
TLP
AMBER
Data Type
-- choose data type --
Data
Data: 8.8.8.8, test.com
Cancel
Start
DNSDB Passive DNS query for Domain Names : Provides history records for a domain
Applies to:
domain
DNSDB_NameHistory (Version: 1.0)
Run
DNSDB Passive DNS query for domain/host name history : Provides history records for an domain/host
Applies to:
fqdn

CORTEX

Cortex | + New Analysis | Analyzers | Jobs

Job details

< Back to list

PhishingInitiative_Lookup_1_0

Artifact
[URL] hxxps://www[.]wuichbinbereits-kunde[.]net/

Date
9 minutes ago

Status
Success

Job report


```
{
  "artifacts": [
    {
      "type": "url",
      "value": "https://www.wuichbinbereits-kunde.net"
    },
    {
      "type": "domain",
      "value": "www.wuichbinbereits-kunde.net"
    }
  ],
  "full": {
    "url": "https://www.wuichbinbereits-kunde.net/",
    "tag": 1,
    "tag_label": "phishing"
  },
  "success": true,
  "summary": {
    "status": "phishing"
  }
}
```

Jobs

Data Types

- ip
- domain
- fqdn
- file
- url
- mail
- other
- hash

Analyzers

- DNSDB_IPHistory
- DNSDB_DomainName
- DNSDB_NameHistory
- Msg_Parser
- Fortiguard_URLCategory
- File_Info
- MaxMind_GeoIP
- PhishTank_CheckURL
- PhishingInitiative_Lookup
- DomainTools_ReverseWhois

Search for observable data

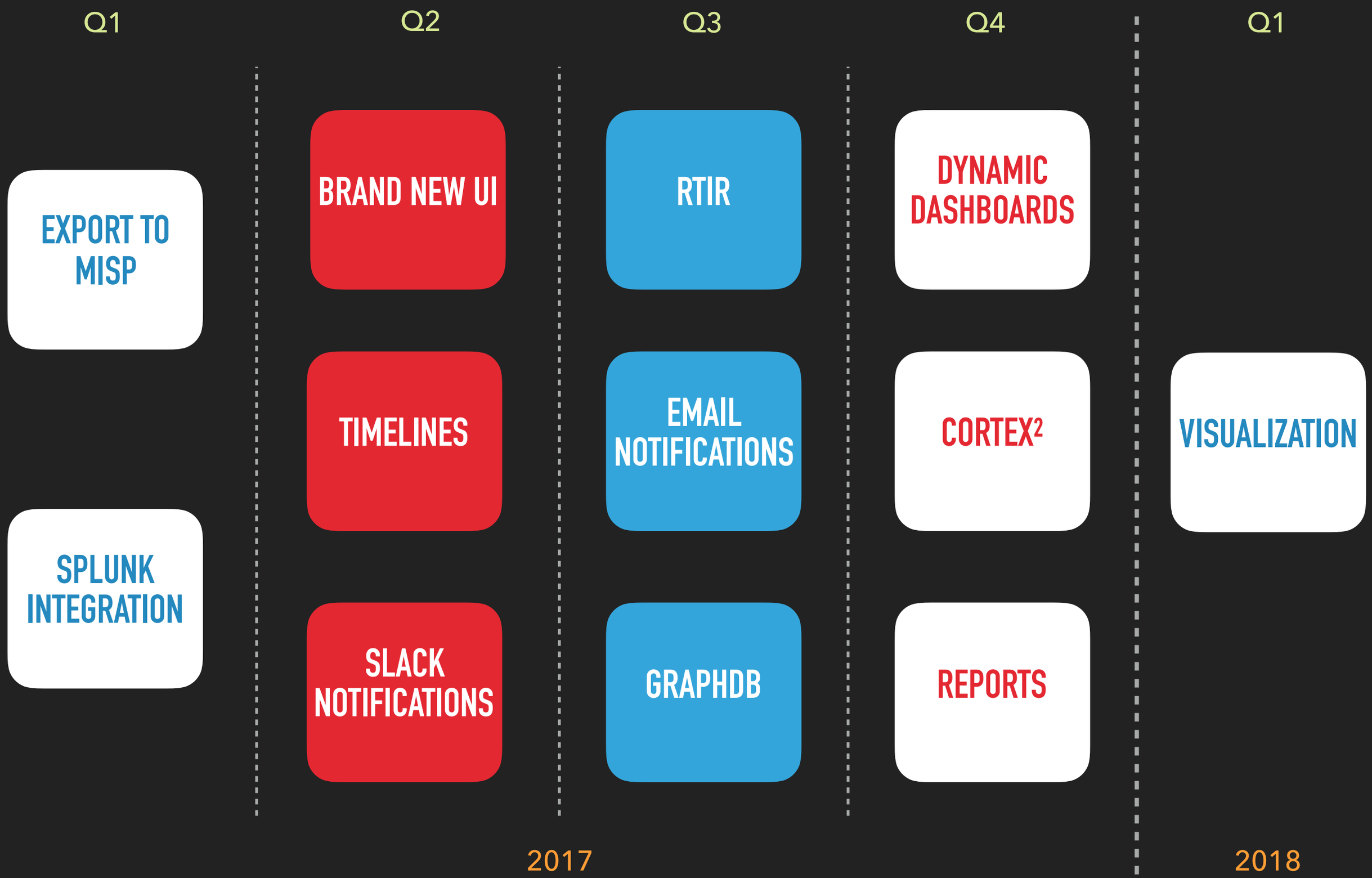
List of existing jobs

Status	Analyzer	Date	Artifact	Data Type
Success	VirusTotal_GetReport_2_0	9 minutes ago	1234057937[.]exe[.]dr	file
Success	DomainTools_WhoisHistory_1_0	a day ago	kingwestvillage[.]com	domain
Success	DomainTools_WhoisLookup_1_0	a day ago	kingwestvillage[.]com	domain
Success	VirusTotal_Scan_2_0	a day ago	blah[.]txt	file
Success	VirusTotal_GetReport_2_0	a day ago	217ffd200fe90c89a06782385fb0615d	hash

WHERE WE ARE HEADED

ROADMAP

MILESTONES


Q1
Q2
Q3
Q4
Q1
EXPORT TO MISP
SPLUNK INTEGRATION
BRAND NEW UI
TIMELINES
SLACK NOTIFICATIONS
RTIR
EMAIL NOTIFICATIONS
GRAPHDB
DYNAMIC DASHBOARDS
CORTEX2
REPORTS
VISUALIZATION
2017
2018

CORTEX²

- Authentication, subscription and analyzer configuration support
- Painless analyzer development
- Analyzers will be provided as dockers
- Rate-limiting
- Report caching

UPCOMING CONNECTORS AND ANALYZERS

CONNECTORS

- ZEROFOX
- DIGITAL SHADOWS
- SPLUNK (ALERTS)
- MISP (EXPORTS)

ANALYZERS

- SPLUNK (SEARCH)
- MISP (SEARCH)
- PASSIVETOTAL
- JOE SANDBOX

THEHIVE PROJECT / https://thehive-project.org/

- Thomas Franco
- Saâd Kadhi
- Jérôme Leonard
- Contributors
  - Nabil Adouani
  - Eric Capuano
  - CERT-BDF