TheHive

OSSIR / 2017-07-11

PUBLIC / TLP:WHITE

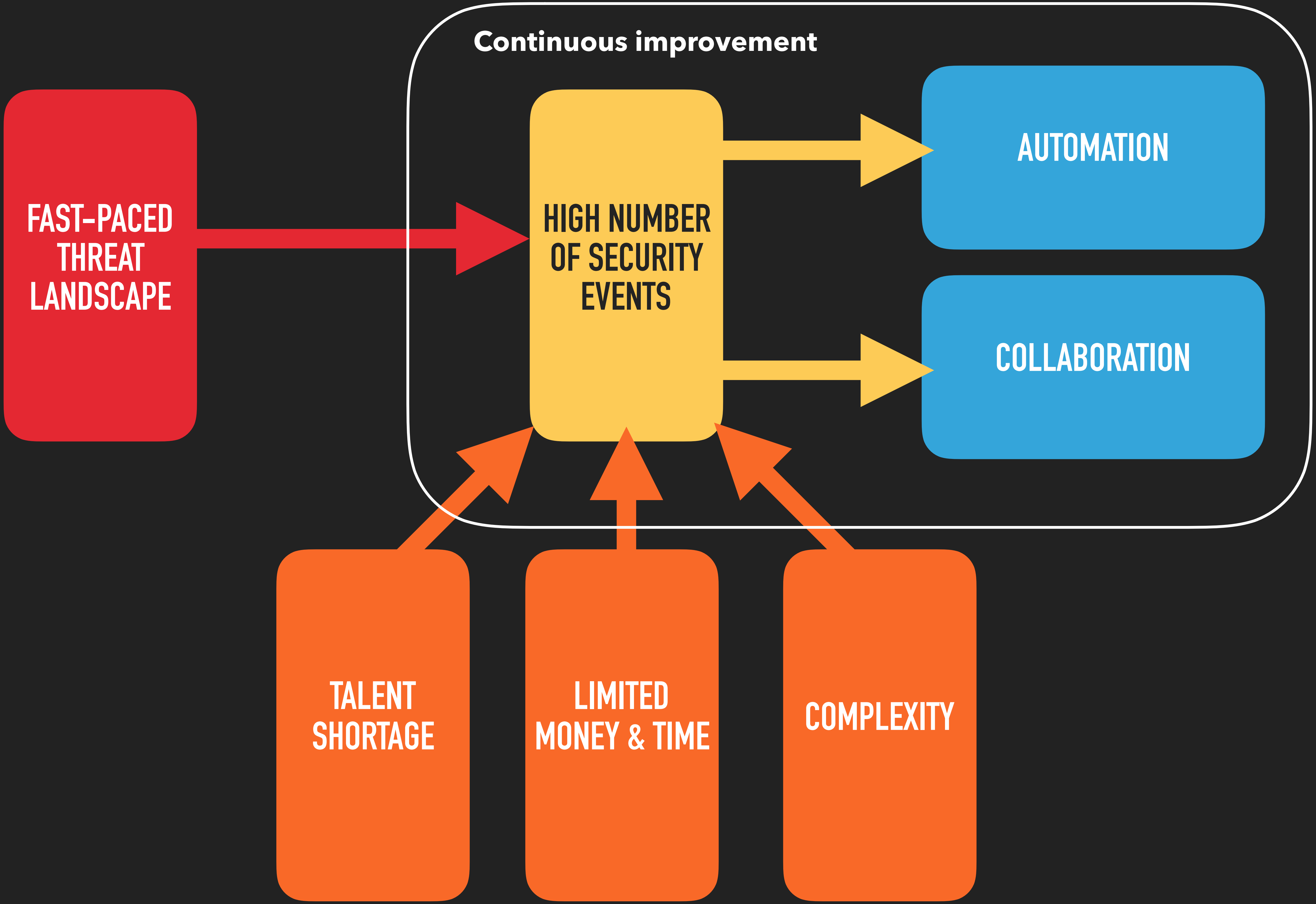
A SCALABLE, OPEN SOURCE AND FREE INCIDENT RESPONSE PLATFORM

Saâd Kadhi
TheHive Project

THREATS & REACTION

OBSERVATIONS

DRIVING DOWN THE TIME TO REACT



DIGITAL FORENSICS AND INCIDENT RESPONSE

- DFIR is a team work
- Mantra: 'with enough eyeballs, skills and mindsets, all threats are shallow'
- DFIR is a set of processes
- We shall seek to drive the 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

HOW TO GET THERE?

SPECS

AUTOMATION & COLLABORATION

- 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 an 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

3 YEARS AGO…

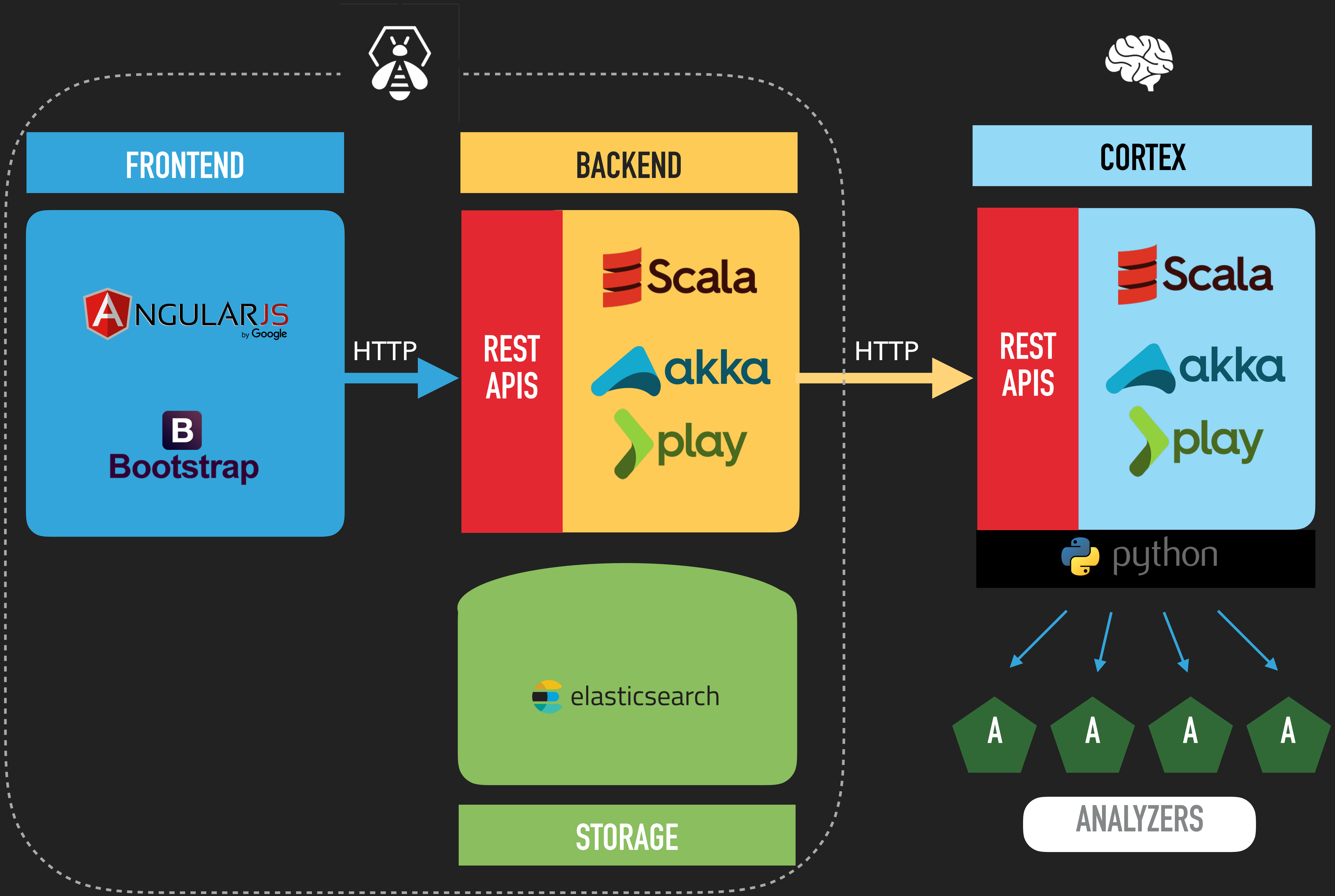
- Hunting for a solution started in early 2014
- Solutions existed but none completely fulfilled the requirements
- Excel/OneNote, AbuseHelper, RTIR, MISP, CIF, Resilient Systems…
- Build or buy? Build

LEARNING FROM BEES

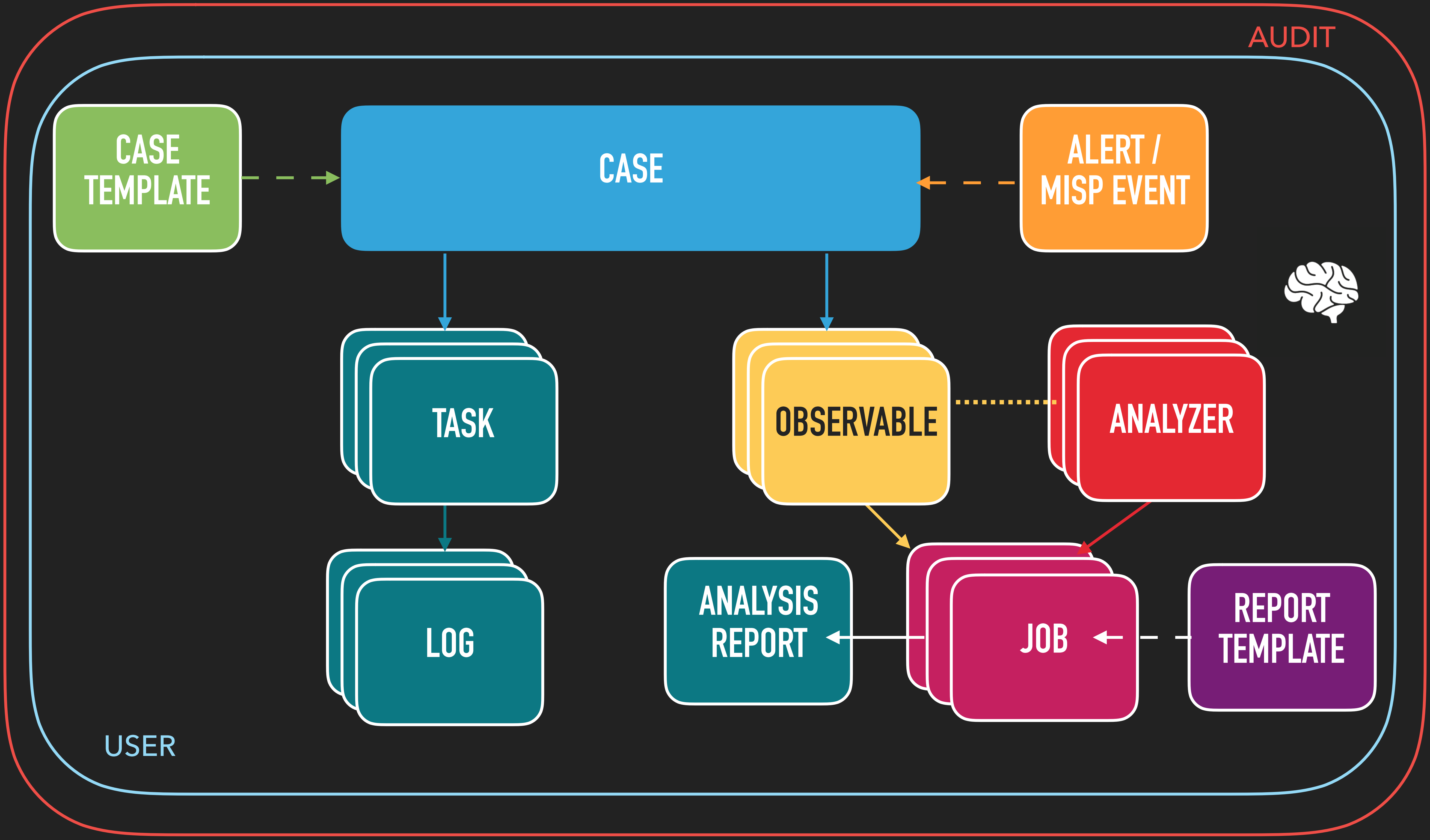
THEHIVE

- 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


AUDIT
CASE TEMPLATE
CASE
ALERT / MISP EVENT
TASK
OBSERVABLE
ANALYZER
LOG
ANALYSIS REPORT
JOB
REPORT TEMPLATE
USER

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

Cortex

- 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

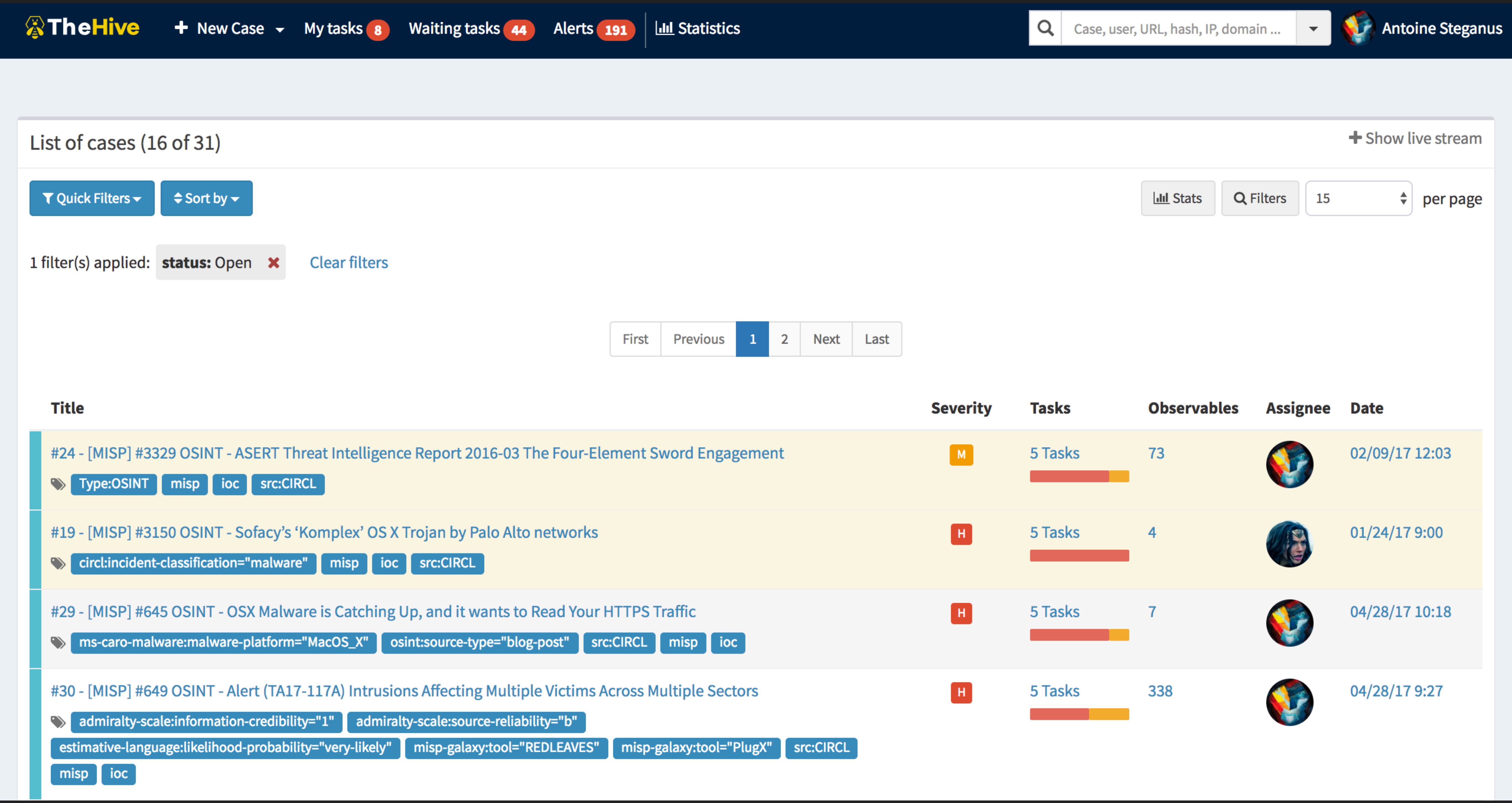
24 ANALYZERS (AND MORE ARE COMING)

PASSIVETOTAL	FORTIGUARD URL CATEGORY	HIPPOCAMPE	MAXMIND	SPLUNK SEARCH
CIRCL PSSL	CIRCL PDNS	GOOGLE SAFE BROWSING	JOE SANDBOX	CUCKOO
MISP SEARCH	VIRUSTOTAL	DNSDB	VMRAY	MCAFEE ATD
DOMAINTOOLS	ABUSE FINDER	YARA	FIREHOL	IRMA
FILEINFO	NESSUS	PHISHING INITIATIVE	CERT.AT PDNS	WHOISXMLAPI
OUTLOOK MSG PARSER	OTXQUERY	PHISHTANK	HIPPOCAMPE	FIREEYE AX
INTELMQ	FAME	HYBRID ANALYSIS	YETI	C1FAPP

SHOW TIME

DEMO?

MAIN VIEW



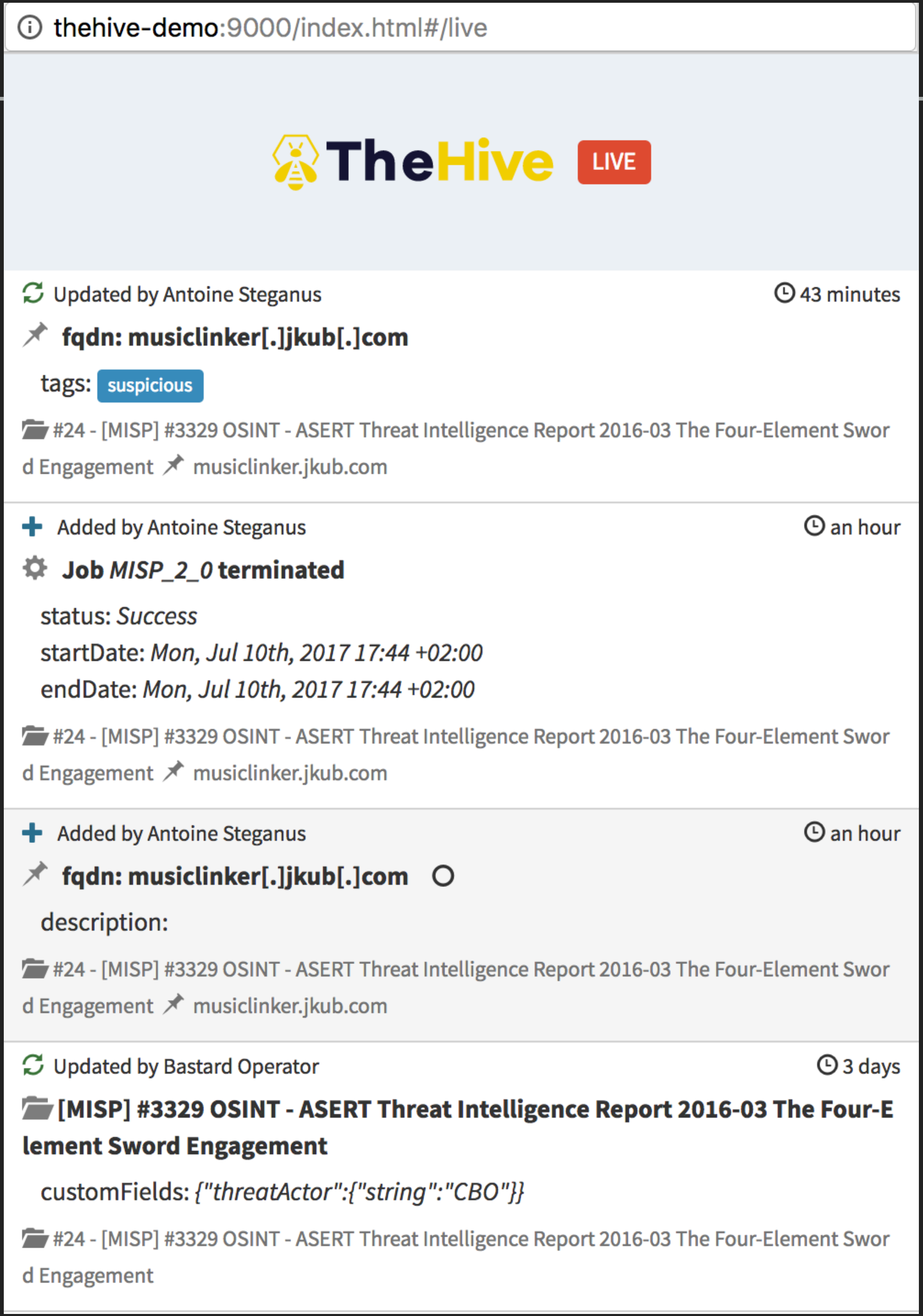
List of cases (16 of 31)

15 per page

1 filter(s) applied: **status:** Open ✖ Clear filters

Title	Severity	Tasks	Observables	Assignee	Date
#24 - [MISP] #3329 OSINT - ASERT Threat Intelligence Report 2016-03 The Four-Element Sword Engagement Type:OSINT misp ioc src:CIRCL	M	5 Tasks	73		02/09/17 12:03
#19 - [MISP] #3150 OSINT - Sofacy's 'Komplex' OS X Trojan by Palo Alto networks circl:incident-classification="malware" misp ioc src:CIRCL	H	5 Tasks	4		01/24/17 9:00
#29 - [MISP] #645 OSINT - OSX Malware is Catching Up, and it wants to Read Your HTTPS Traffic ms-caro-malware:malware-platform="MacOS_X" osint:source-type="blog-post" src:CIRCL misp ioc	H	5 Tasks	7		04/28/17 10:18
#30 - [MISP] #649 OSINT - Alert (TA17-117A) Intrusions Affecting Multiple Victims Across Multiple Sectors admiralty-scale:information-credibility="1" admiralty-scale:source-reliability="b" estimative-language:likelihood-probability="very-likely" misp-galaxy:tool="REDLEAVES" misp-galaxy:tool="PlugX" src:CIRCL misp ioc	H	5 Tasks	338		04/28/17 9:27

LIVE STREAM



Updated by Antoine Steganus 43 minutes

fqdn: musiclinker[.]jkub[.]com

tags: suspicious

#24 - [MISP] #3329 OSINT - ASERT Threat Intelligence Report 2016-03 The Four-Element Sword Engagement musiclinker.jkub.com

Added by Antoine Steganus an hour

Job *MISP_2_0* terminated

status: *Success*
startDate: *Mon, Jul 10th, 2017 17:44 +02:00*
endDate: *Mon, Jul 10th, 2017 17:44 +02:00*

#24 - [MISP] #3329 OSINT - ASERT Threat Intelligence Report 2016-03 The Four-Element Sword Engagement musiclinker.jkub.com

Added by Antoine Steganus an hour

fqdn: musiclinker[.]jkub[.]com ○

description:

#24 - [MISP] #3329 OSINT - ASERT Threat Intelligence Report 2016-03 The Four-Element Sword Engagement musiclinker.jkub.com

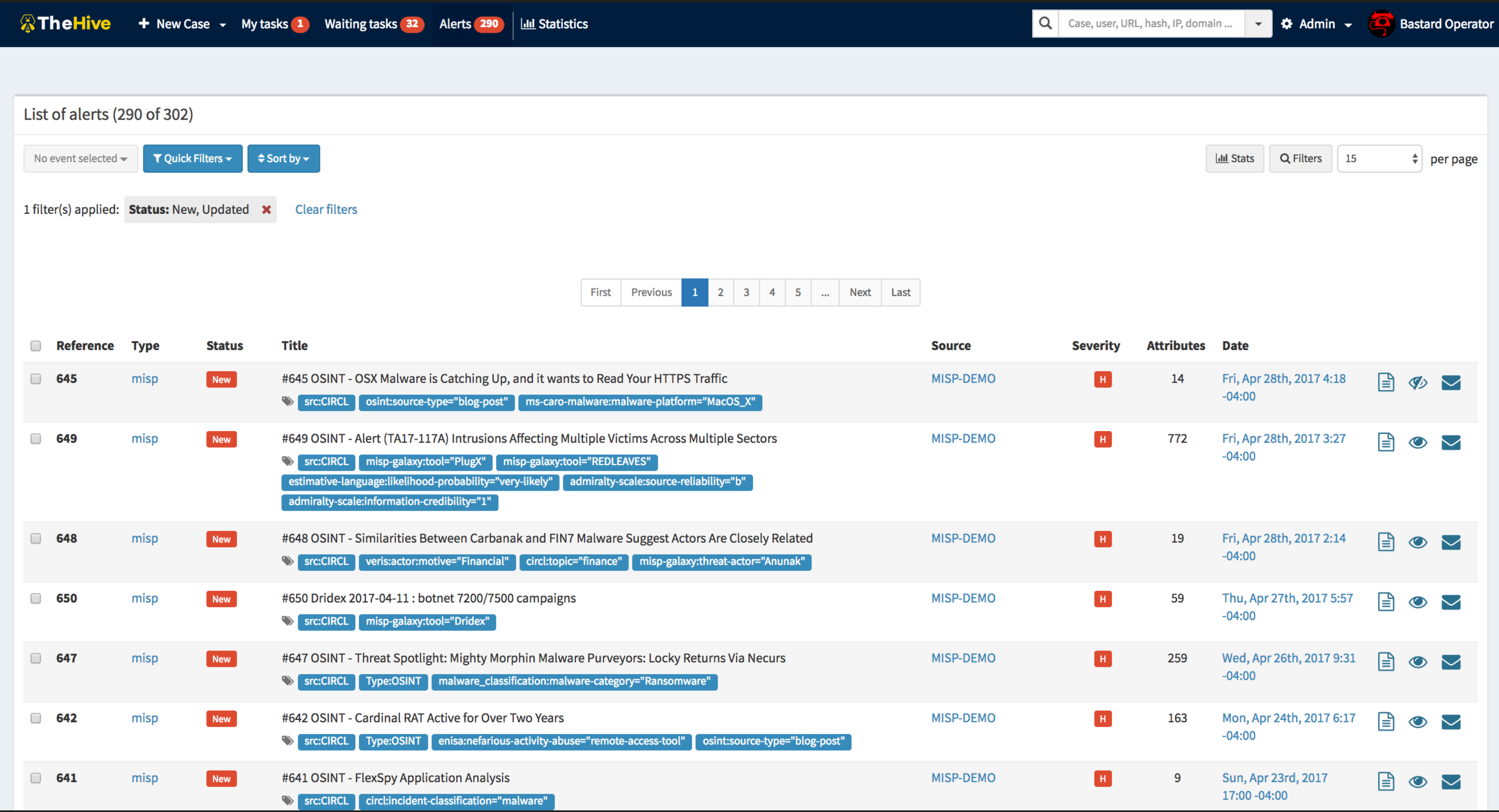
Updated by Bastard Operator 3 days

[MISP] #3329 OSINT - ASERT Threat Intelligence Report 2016-03 The Four-Element Sword Engagement

customFields: *{"threatActor":{"string":"CBO"}}*

#24 - [MISP] #3329 OSINT - ASERT Threat Intelligence Report 2016-03 The Four-Element Sword Engagement

ALERT PANEL

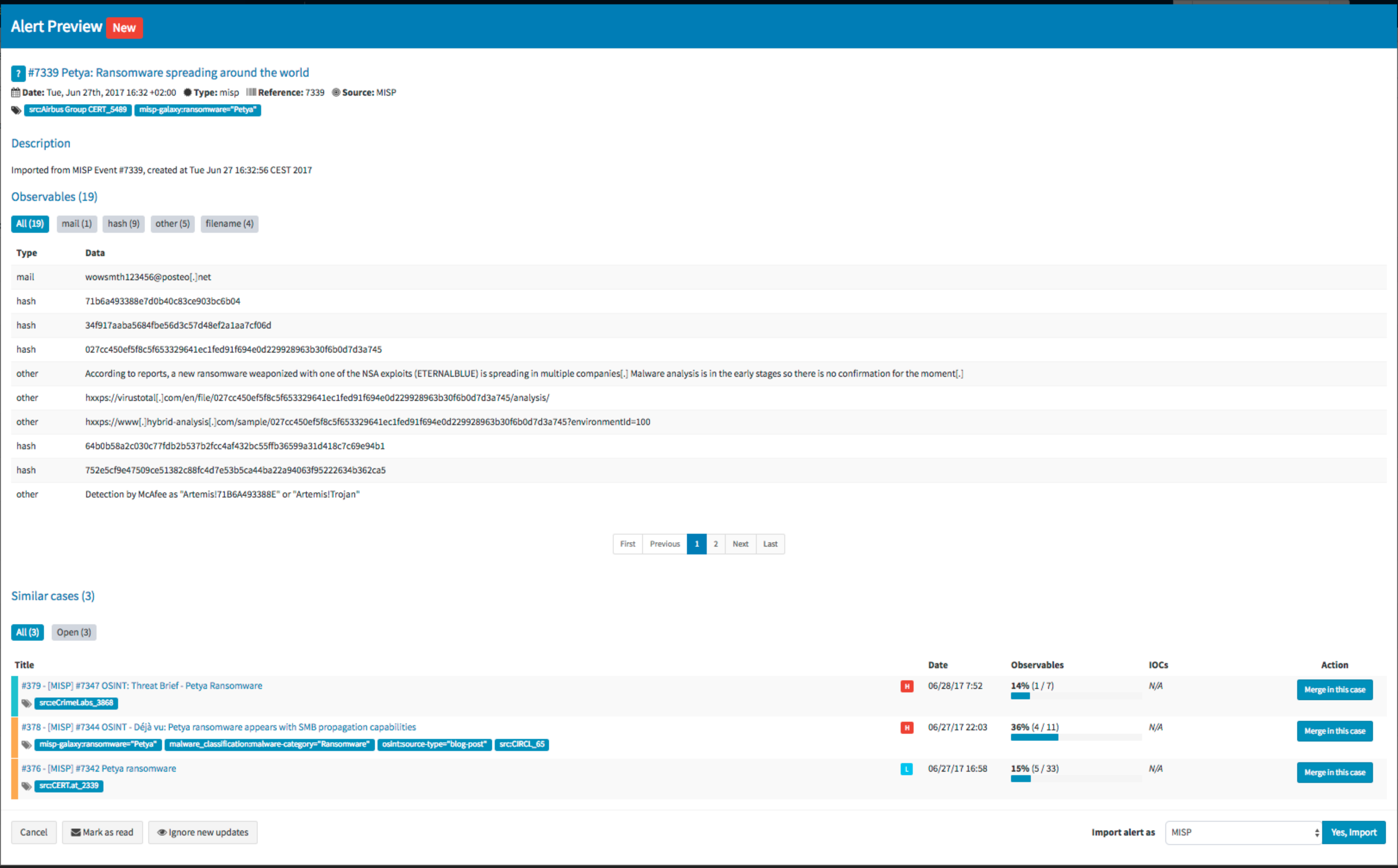


List of alerts (290 of 302)

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

□	Reference	Type	Status	Title	Source	Severity	Attributes	Date
□	645	misp	New	#645 OSINT - OSX Malware is Catching Up, and it wants to Read Your HTTPS Traffic src:CIRCL osint:source-type="blog-post" ms-caro-malware:malware-platform="MacOS_X"	MISP-DEMO	H	14	Fri, Apr 28th, 2017 4:18 -04:00
□	649	misp	New	#649 OSINT - Alert (TA17-117A) Intrusions Affecting Multiple Victims Across Multiple Sectors src:CIRCL misp-galaxy:tool="PlugX" misp-galaxy:tool="REDLEAVES" estimative-language:likelihood-probability="very-likely" admiralty-scale:source-reliability="b" admiralty-scale:information-credibility="1"	MISP-DEMO	H	772	Fri, Apr 28th, 2017 3:27 -04:00
□	648	misp	New	#648 OSINT - Similarities Between Carbanak and FIN7 Malware Suggest Actors Are Closely Related src:CIRCL veris:actor:motive="Financial" circl:topic="finance" misp-galaxy:threat-actor="Anunak"	MISP-DEMO	H	19	Fri, Apr 28th, 2017 2:14 -04:00
□	650	misp	New	#650 Dridex 2017-04-11 : botnet 7200/7500 campaigns src:CIRCL misp-galaxy:tool="Dridex"	MISP-DEMO	H	59	Thu, Apr 27th, 2017 5:57 -04:00
□	647	misp	New	#647 OSINT - Threat Spotlight: Mighty Morphin Malware Purveyors: Locky Returns Via Necurs src:CIRCL Type:OSINT malware_classification:malware-category="Ransomware"	MISP-DEMO	H	259	Wed, Apr 26th, 2017 9:31 -04:00
□	642	misp	New	#642 OSINT - Cardinal RAT Active for Over Two Years src:CIRCL Type:OSINT enisa:nefarious-activity-abuse="remote-access-tool" osint:source-type="blog-post"	MISP-DEMO	H	163	Mon, Apr 24th, 2017 6:17 -04:00
□	641	misp	New	#641 OSINT - FlexSpy Application Analysis src:CIRCL circl:incident-classification="malware"	MISP-DEMO	H	9	Sun, Apr 23rd, 2017 17:00 -04:00

ALERT PANEL



Alert Preview New

? #7339 Petya: Ransomware spreading around the world

Date: Tue, Jun 27th, 2017 16:32 +02:00 **Type:** misp **Reference:** 7339 **Source:** MISP

src:Airbus Group CERT_5489 misp-galaxy:ransomware="Petya"

Description

Imported from MISP Event #7339, created at Tue Jun 27 16:32:56 CEST 2017

Observables (19)

All (19) mail (1) hash (9) other (5) filename (4)

Type	Data
mail	wowsmth123456@posteo[.]net
hash	71b6a493388e7d0b40c83ce903bc6b04
hash	34f917aaba5684fbe56d3c57d48ef2a1aa7cf06d
hash	027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745
other	According to reports, a new ransomware weaponized with one of the NSA exploits (ETERNALBLUE) is spreading in multiple companies[.] Malware analysis is in the early stages so there is no confirmation for the moment[.]
other	hxxps://virustotal[.]com/en/file/027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745/analysis/
other	hxxps://www[.]hybrid-analysis[.]com/sample/027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745?environmentId=100
hash	64b0b58a2c030c77fdb2b537b2fcc4af432bc55ffb36599a31d418c7c69e94b1
hash	752e5cf9e47509ce51382c88fc4d7e53b5ca44ba22a94063f95222634b362ca5
other	Detection by McAfee as "Artemis!71B6A493388E" or "Artemis!Trojan"

First Previous 1 2 Next Last

Similar cases (3)

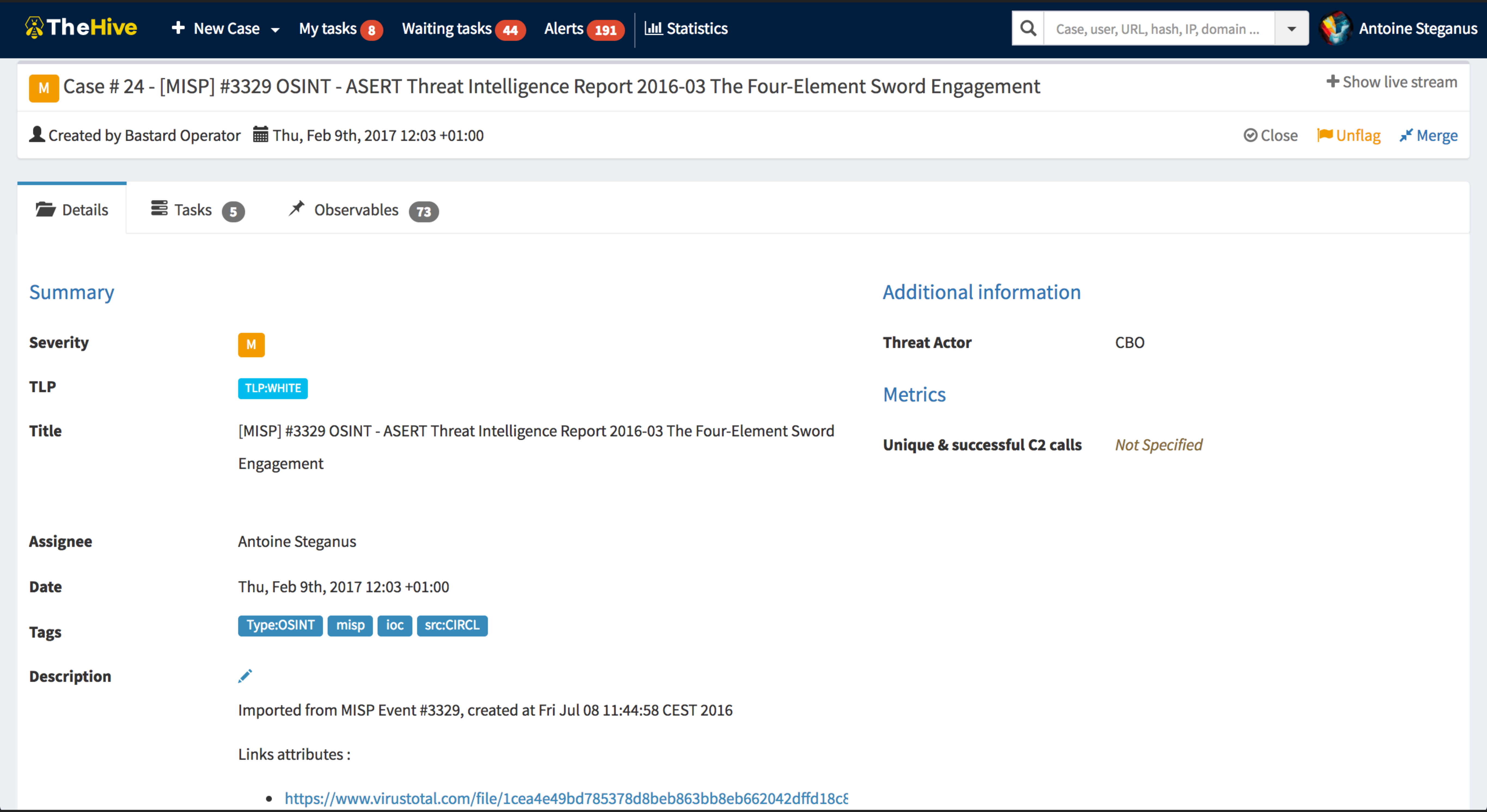
All (3) Open (3)

Title		Date	Observables	IOCs	Action
#379 - [MISP] #7347 OSINT: Threat Brief - Petya Ransomware src:eCrimeLabs_3868	H	06/28/17 7:52	14% (1 / 7)	N/A	Merge in this case
#378 - [MISP] #7344 OSINT - Déjà vu: Petya ransomware appears with SMB propagation capabilities misp-galaxy:ransomware="Petya" malware_classification:malware-category="Ransomware" osint:source-type="blog-post" src:CIRCL_65	H	06/27/17 22:03	36% (4 / 11)	N/A	Merge in this case
#376 - [MISP] #7342 Petya ransomware src:CERT.at_2339	L	06/27/17 16:58	15% (5 / 33)	N/A	Merge in this case

Cancel | Mark as read | Ignore new updates

Import alert as MISP | Yes, Import

CASE VIEW



M Case # 24 - [MISP] #3329 OSINT - ASERT Threat Intelligence Report 2016-03 The Four-Element Sword Engagement

Created by Bastard Operator Thu, Feb 9th, 2017 12:03 +01:00

Summary

Severity	M
TLP	TLP:WHITE
Title	[MISP] #3329 OSINT - ASERT Threat Intelligence Report 2016-03 The Four-Element Sword Engagement
Assignee	Antoine Steganus
Date	Thu, Feb 9th, 2017 12:03 +01:00
Tags	Type:OSINT misp ioc src:CIRCL
Description	Imported from MISP Event #3329, created at Fri Jul 08 11:44:58 CEST 2016

Links attributes :

- https://www.virustotal.com/file/1cea4e49bd785378d8beb863bb8eb662042dffd18c8

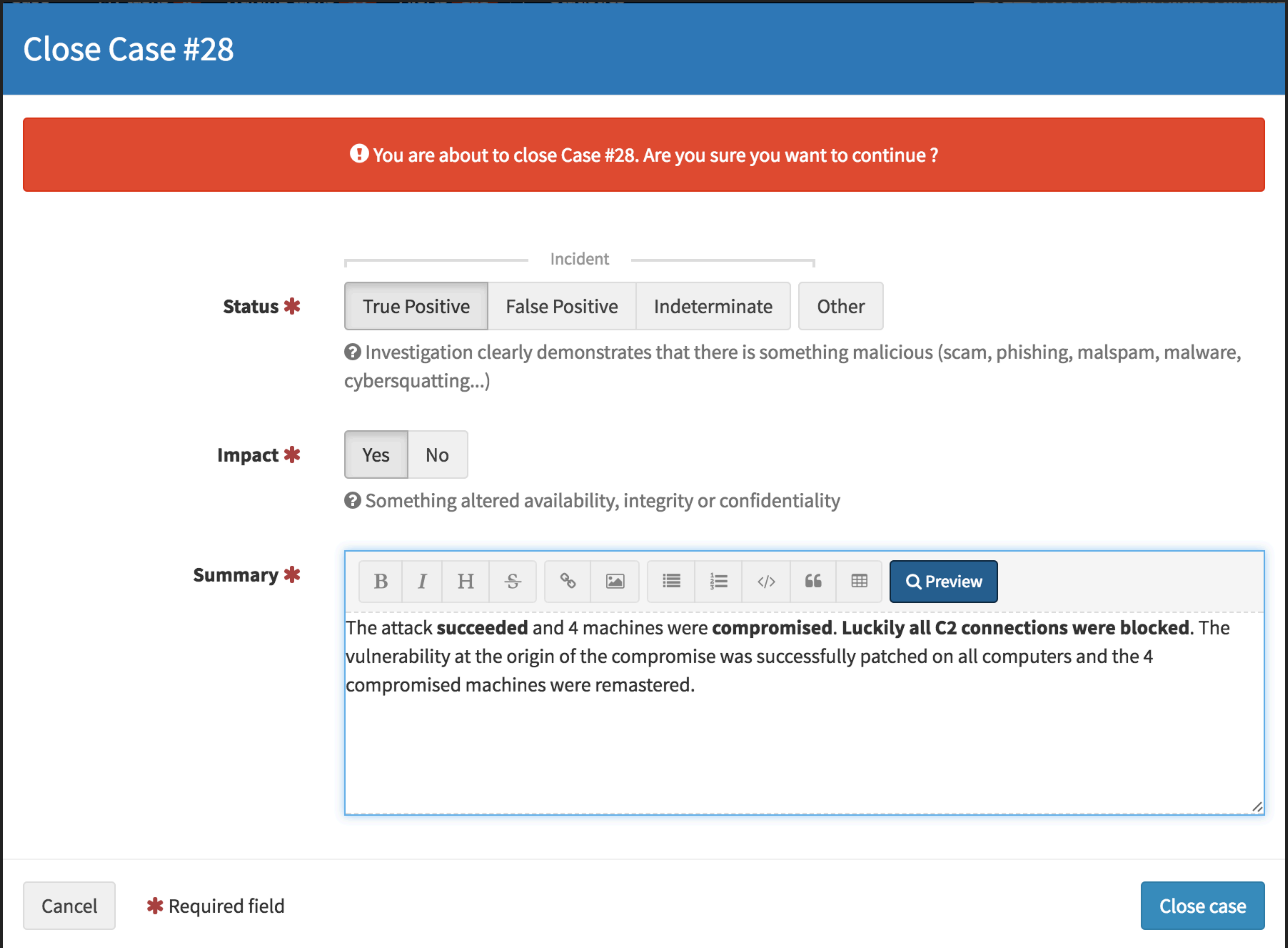
Additional information

Threat Actor	CBO

Metrics

Unique & successful C2 calls	*Not Specified*

CASE VIEW



Close Case #28

You are about to close Case #28. Are you sure you want to continue ?

Status ✱ [✓ True Positive] False Positive Indeterminate Other

Investigation clearly demonstrates that there is something malicious (scam, phishing, malspam, malware, cybersquatting...)

Impact ✱ [✓ Yes] No

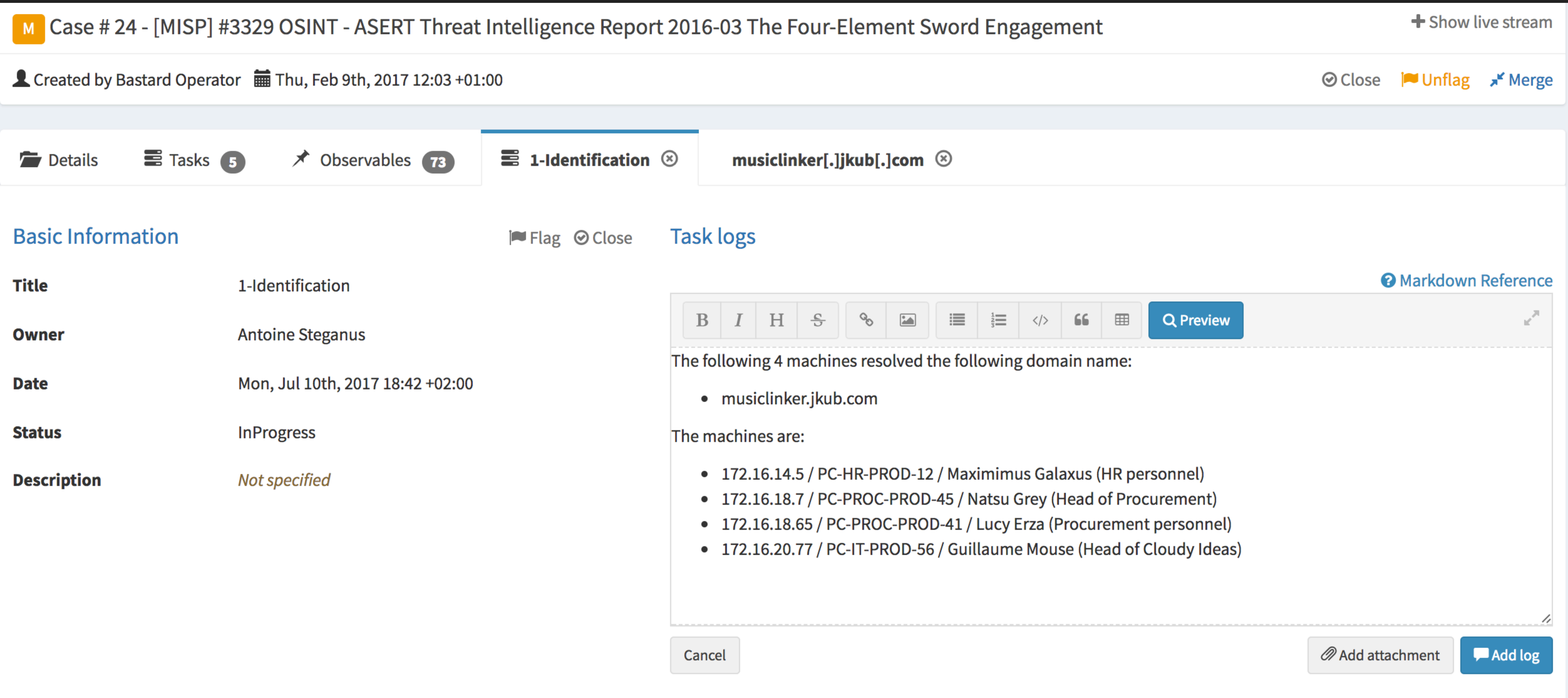
Something altered availability, integrity or confidentiality

Summary ✱

The attack **succeeded** and 4 machines were **compromised**. **Luckily all C2 connections were blocked**. The vulnerability at the origin of the compromise was successfully patched on all computers and the 4 compromised machines were remastered.

✱ Required field

LOG VIEW



Case # 24 - [MISP] #3329 OSINT - ASERT Threat Intelligence Report 2016-03 The Four-Element Sword Engagement

Created by Bastard Operator Thu, Feb 9th, 2017 12:03 +01:00

Basic Information

Title	1-Identification
Owner	Antoine Steganus
Date	Mon, Jul 10th, 2017 18:42 +02:00
Status	InProgress
Description	*Not specified*

Task logs

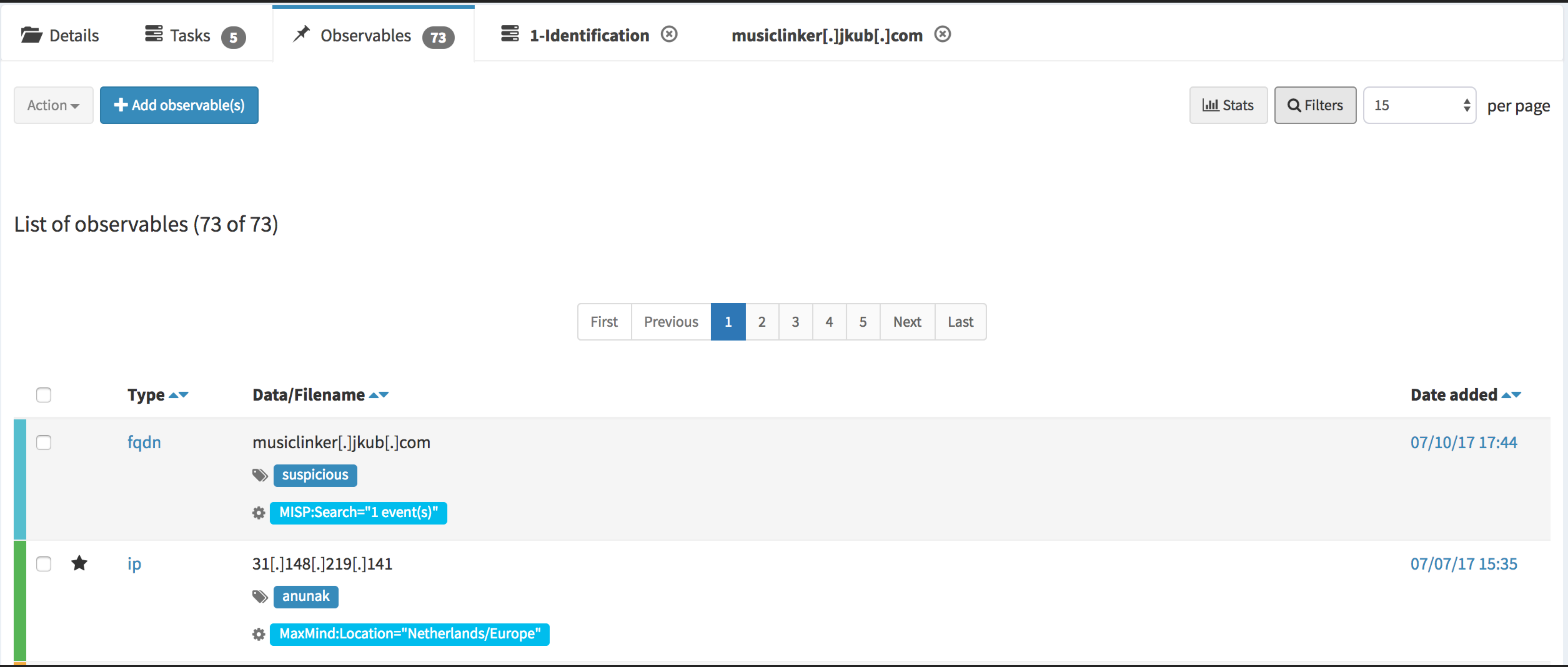
The following 4 machines resolved the following domain name:

- musiclinker.jkub.com

The machines are:

- 172.16.14.5 / PC-HR-PROD-12 / Maximimus Galaxus (HR personnel)
- 172.16.18.7 / PC-PROC-PROD-45 / Natsu Grey (Head of Procurement)
- 172.16.18.65 / PC-PROC-PROD-41 / Lucy Erza (Procurement personnel)
- 172.16.20.77 / PC-IT-PROD-56 / Guillaume Mouse (Head of Cloudy Ideas)

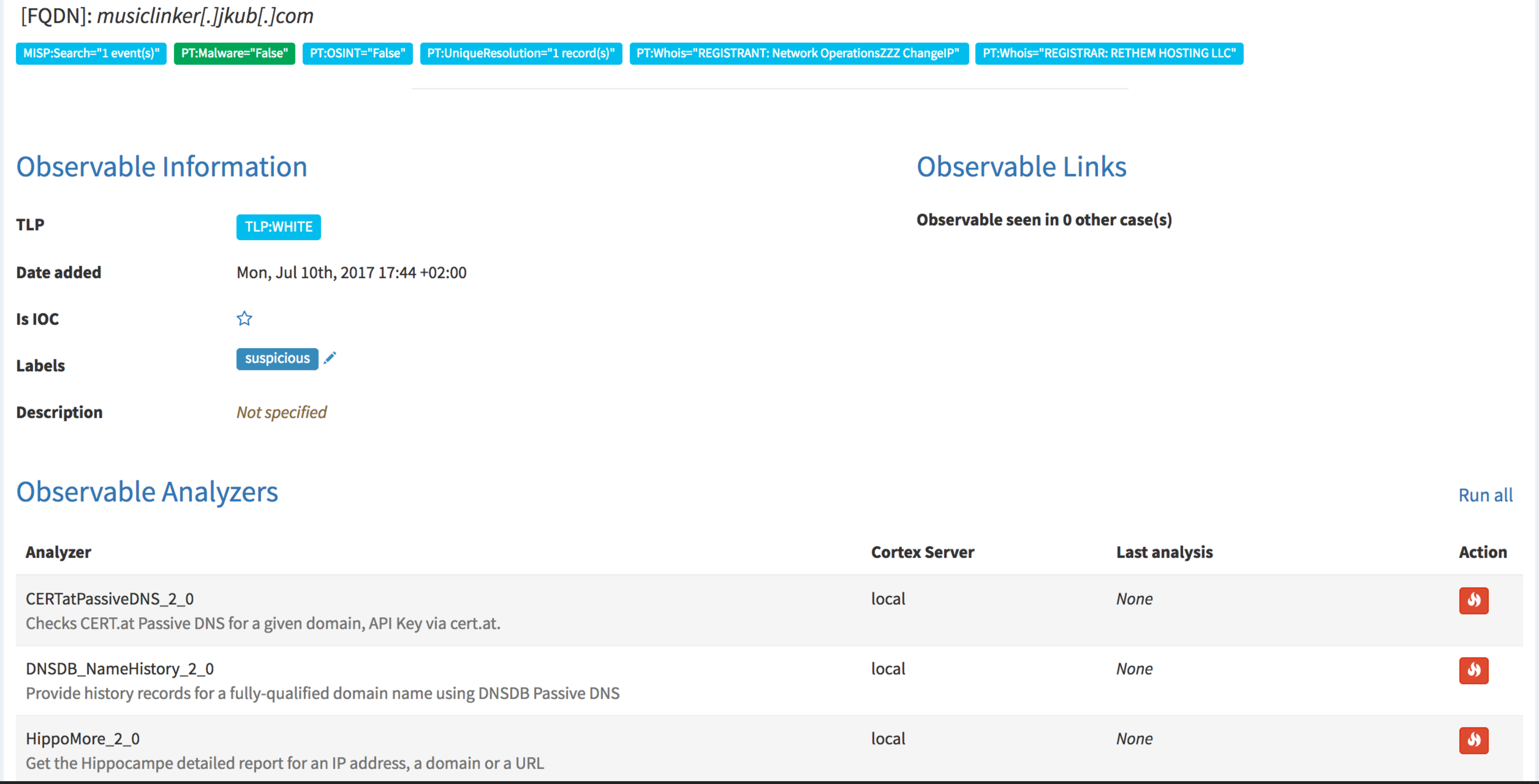
OBSERVABLE VIEW



List of observables (73 of 73)

□		Type	Data/Filename	Date added
□		fqdn	musiclinker[.]jkub[.]com suspicious MISP:Search="1 event(s)"	07/10/17 17:44
□	★	ip	31[.]148[.]219[.]141 anunak MaxMind:Location="Netherlands/Europe"	07/07/17 15:35

OBSERVABLE VIEW



[FQDN]: *musiclinker[.]jkub[.]com*

MISP:Search="1 event(s)" PT:Malware="False" PT:OSINT="False" PT:UniqueResolution="1 record(s)" PT:Whois="REGISTRANT: Network OperationsZZZ ChangeIP" PT:Whois="REGISTRAR: RETHEM HOSTING LLC"

Observable Information

TLP	TLP:WHITE
Date added	Mon, Jul 10th, 2017 17:44 +02:00
Is IOC	☆
Labels	suspicious
Description	*Not specified*

Observable Links

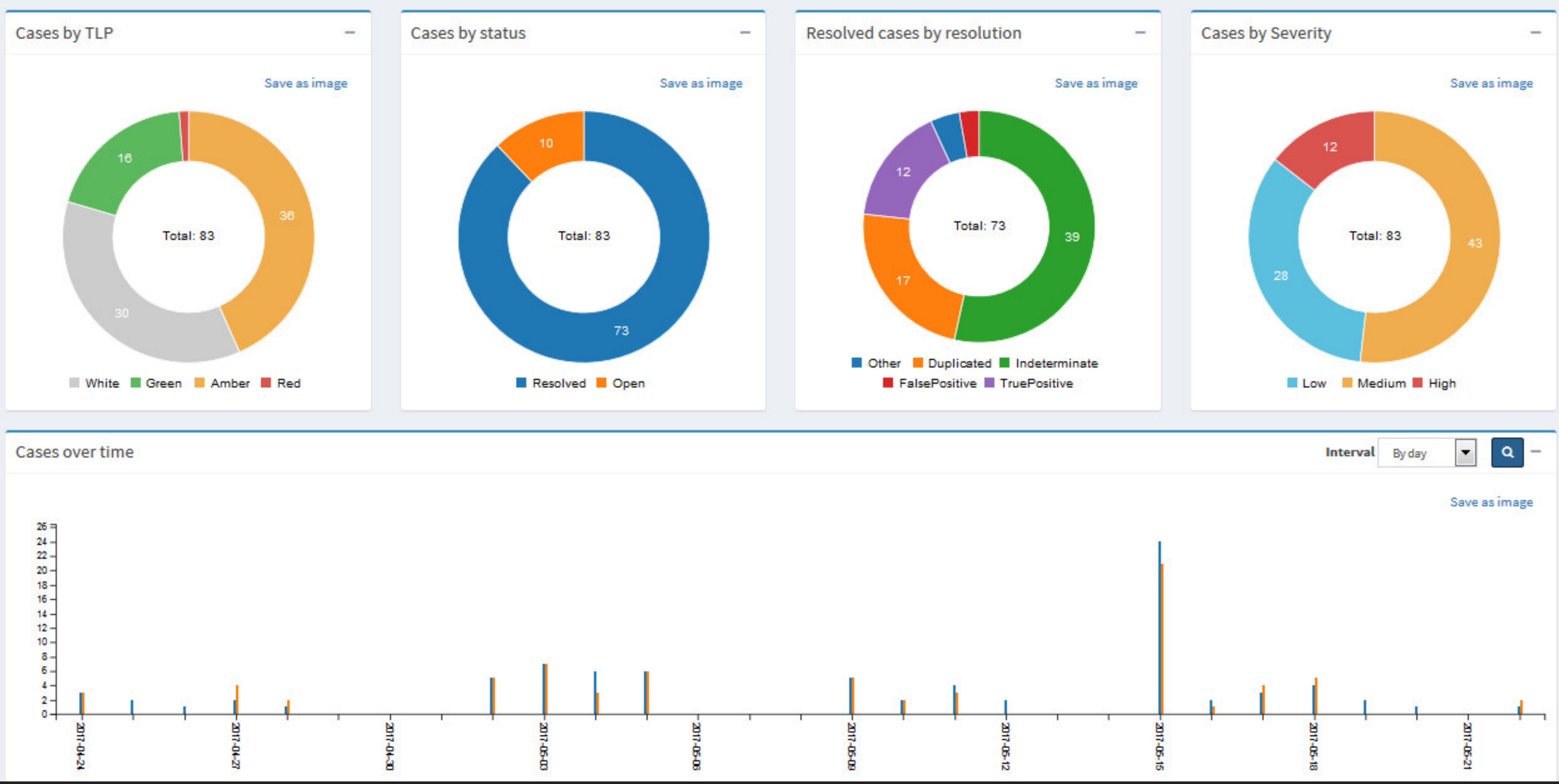
Observable seen in 0 other case(s)

Observable Analyzers

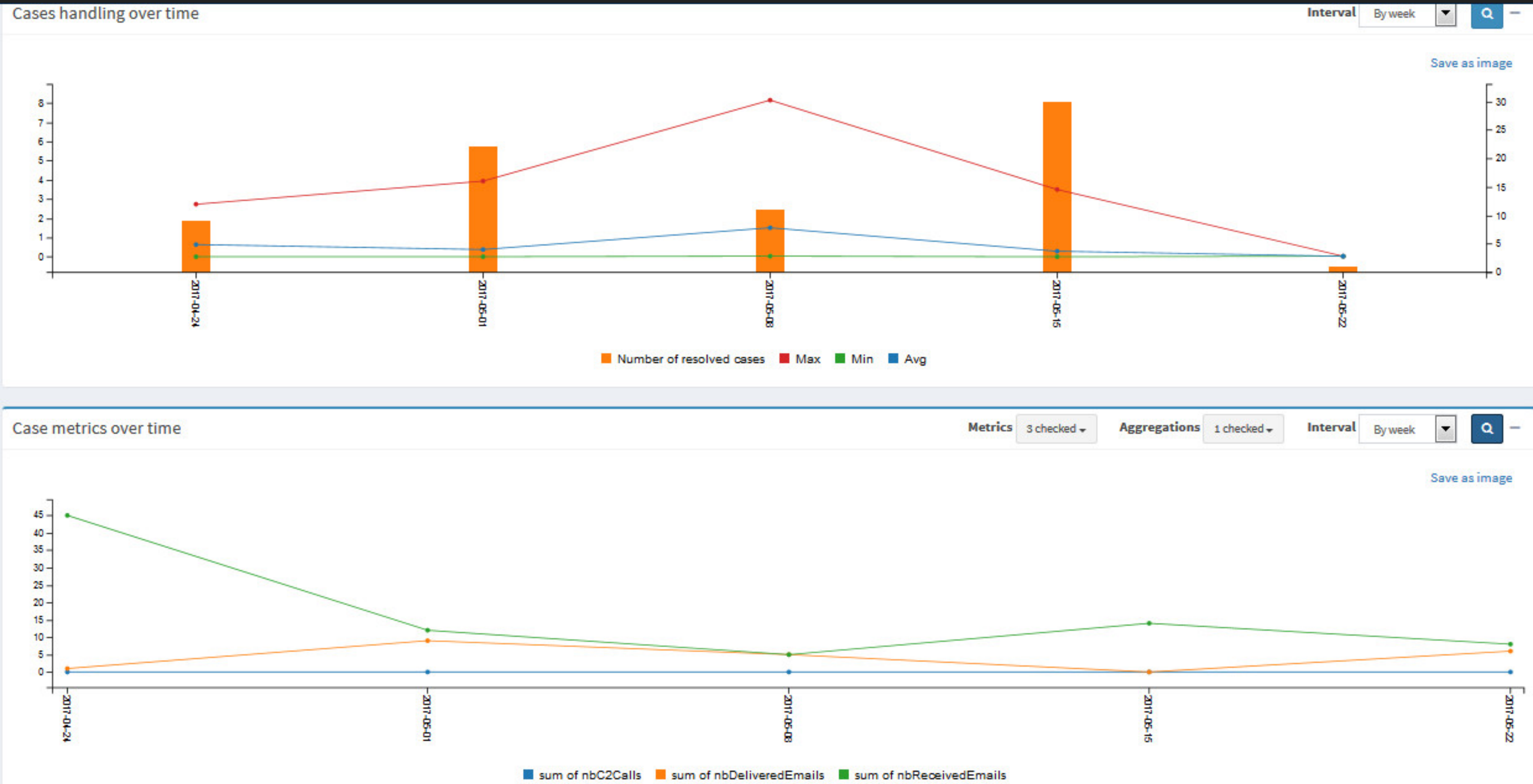
Run all

Analyzer	Cortex Server	Last analysis	Action
CERTatPassiveDNS_2_0 Checks CERT.at Passive DNS for a given domain, API Key via cert.at.	local	*None*	🔥
DNSDB_NameHistory_2_0 Provide history records for a fully-qualified domain name using DNSDB Passive DNS	local	*None*	🔥
HippoMore_2_0 Get the Hippocampe detailed report for an IP address, a domain or a URL	local	*None*	🔥

STATISTICS


Cases by TLP
Save as image
16
36
30
Total: 83
White
Green
Amber
Red
Cases by status
Save as image
10
73
Total: 83
Resolved
Open
Resolved cases by resolution
Save as image
12
17
39
Total: 73
Other
Duplicated
Indeterminate
FalsePositive
TruePositive
Cases by Severity
Save as image
12
28
43
Total: 83
Low
Medium
High
Cases over time
Interval
By day
Save as image
26
24
22
20
18
16
14
12
10
8
6
4
2
0
2017-04-24
2017-04-27
2017-04-30
2017-05-03
2017-05-06
2017-05-09
2017-05-12
2017-05-15
2017-05-18
2017-05-21

STATISTICS



Cases handling over time

Interval By week

Save as image

Case metrics over time

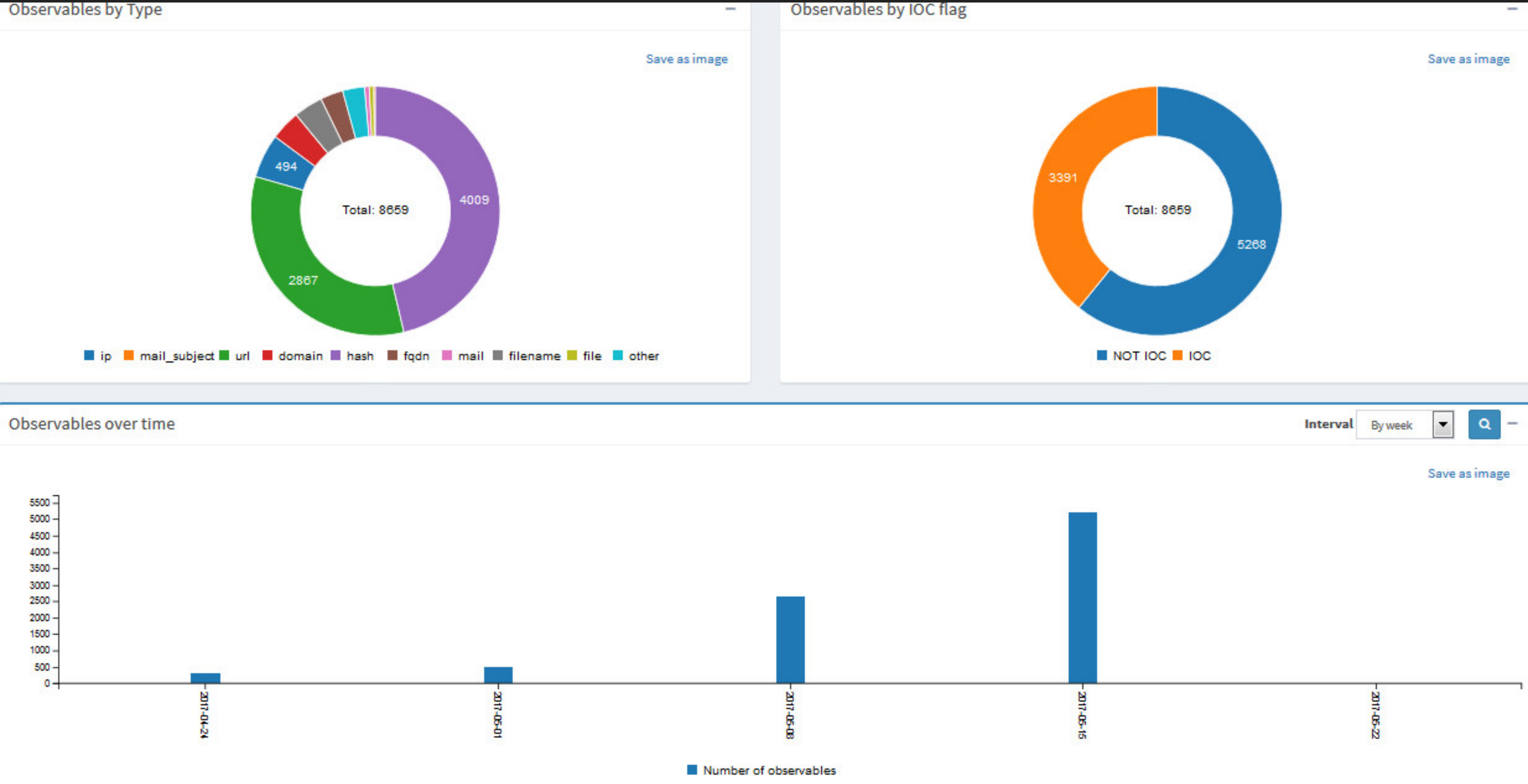
Metrics 3 checked

Aggregations 1 checked

Interval By week

Save as image

STATISTICS



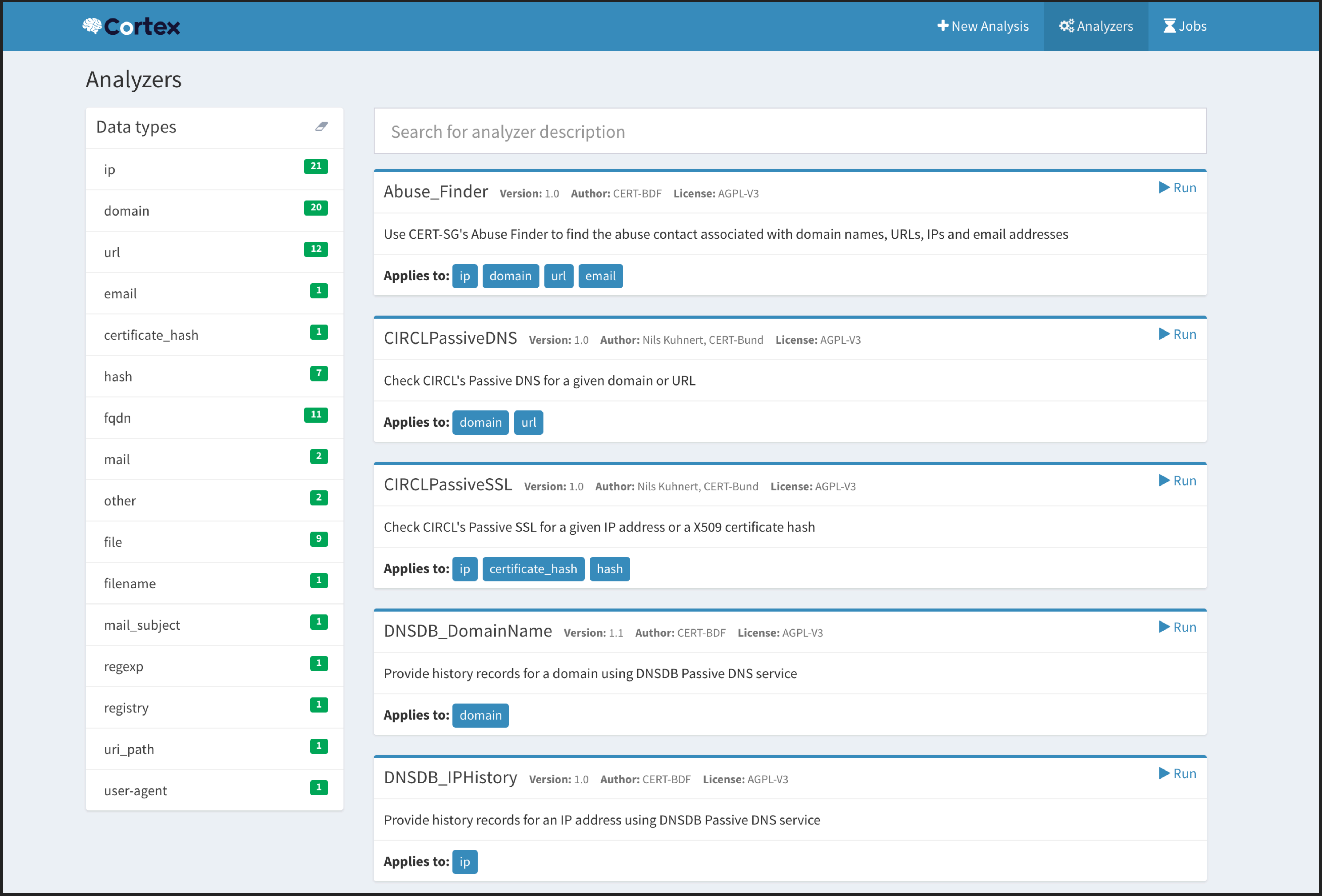
Observables by Type

Observables by IOC flag

Observables over time

Interval: By week

CORTEX



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

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

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

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

Provide history records for a domain using DNSDB Passive DNS service

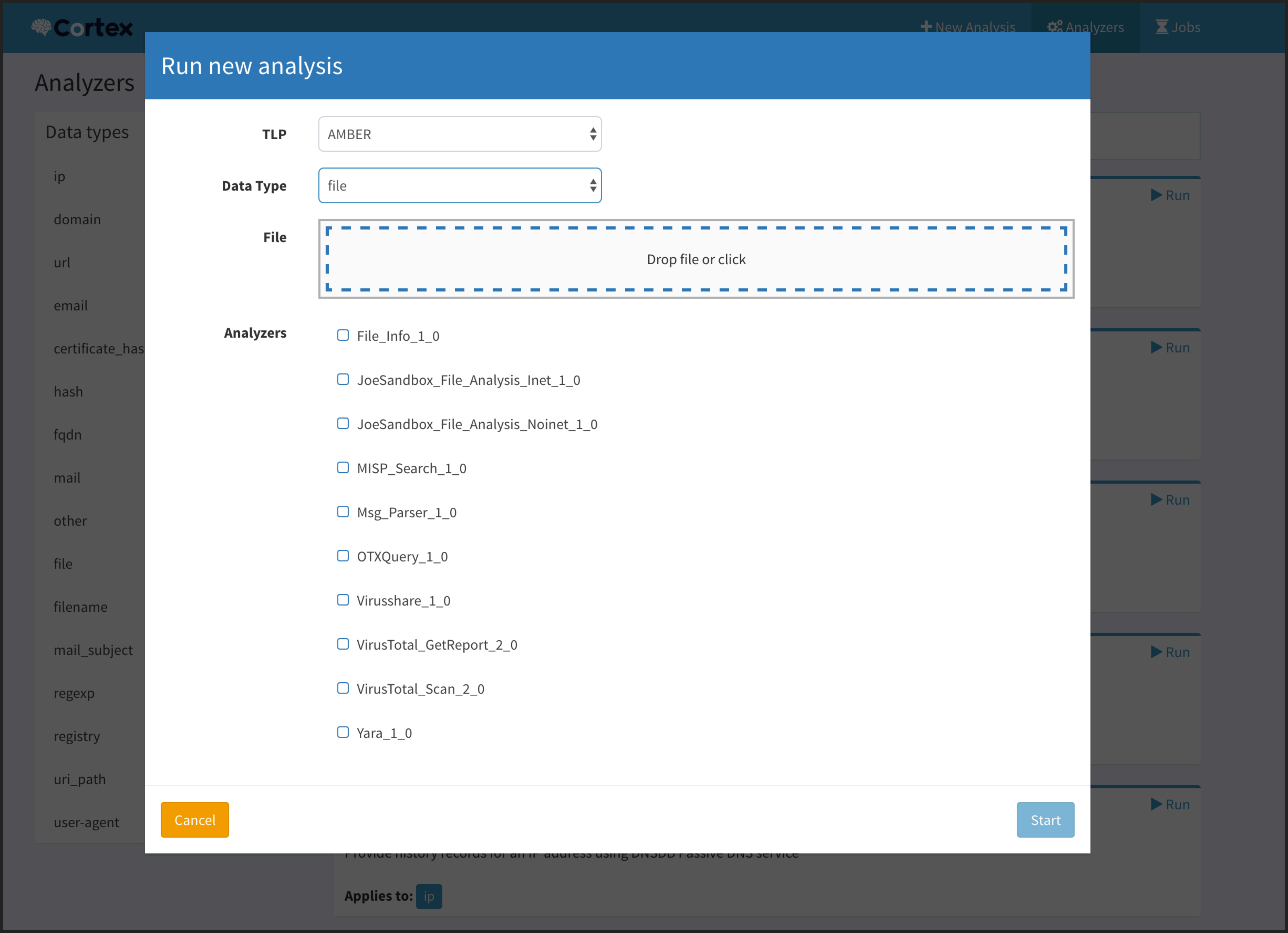
Applies to: domain

DNSDB_IPHistory **Version:** 1.0 **Author:** CERT-BDF **License:** AGPL-V3

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

Applies to: ip

CORTEX



Run new analysis

TLP AMBER

Data Type file

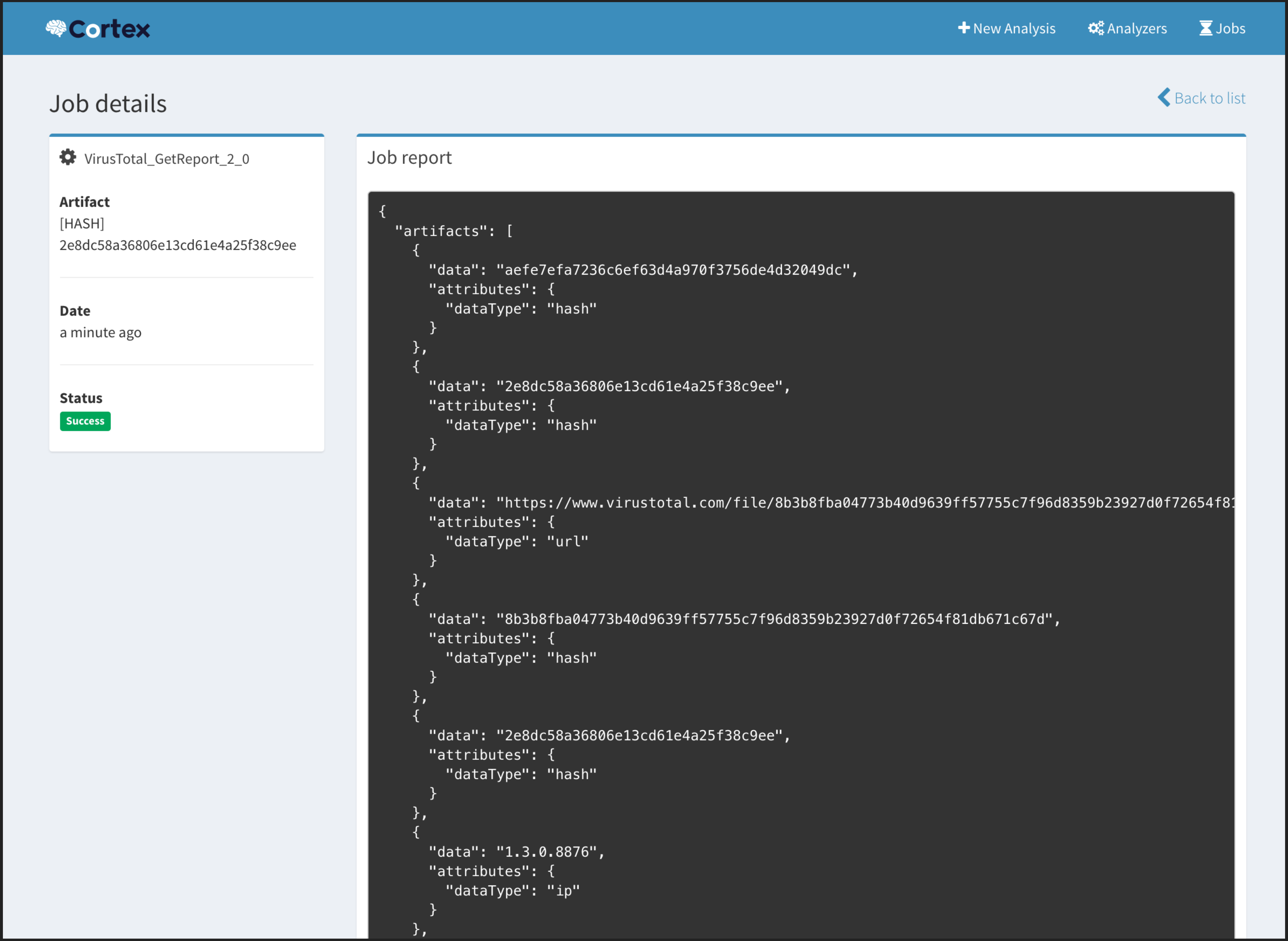
File Drop file or click

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

CORTEX



Job details

VirusTotal_GetReport_2_0

Artifact
[HASH]
2e8dc58a36806e13cd61e4a25f38c9ee

Date
a minute ago

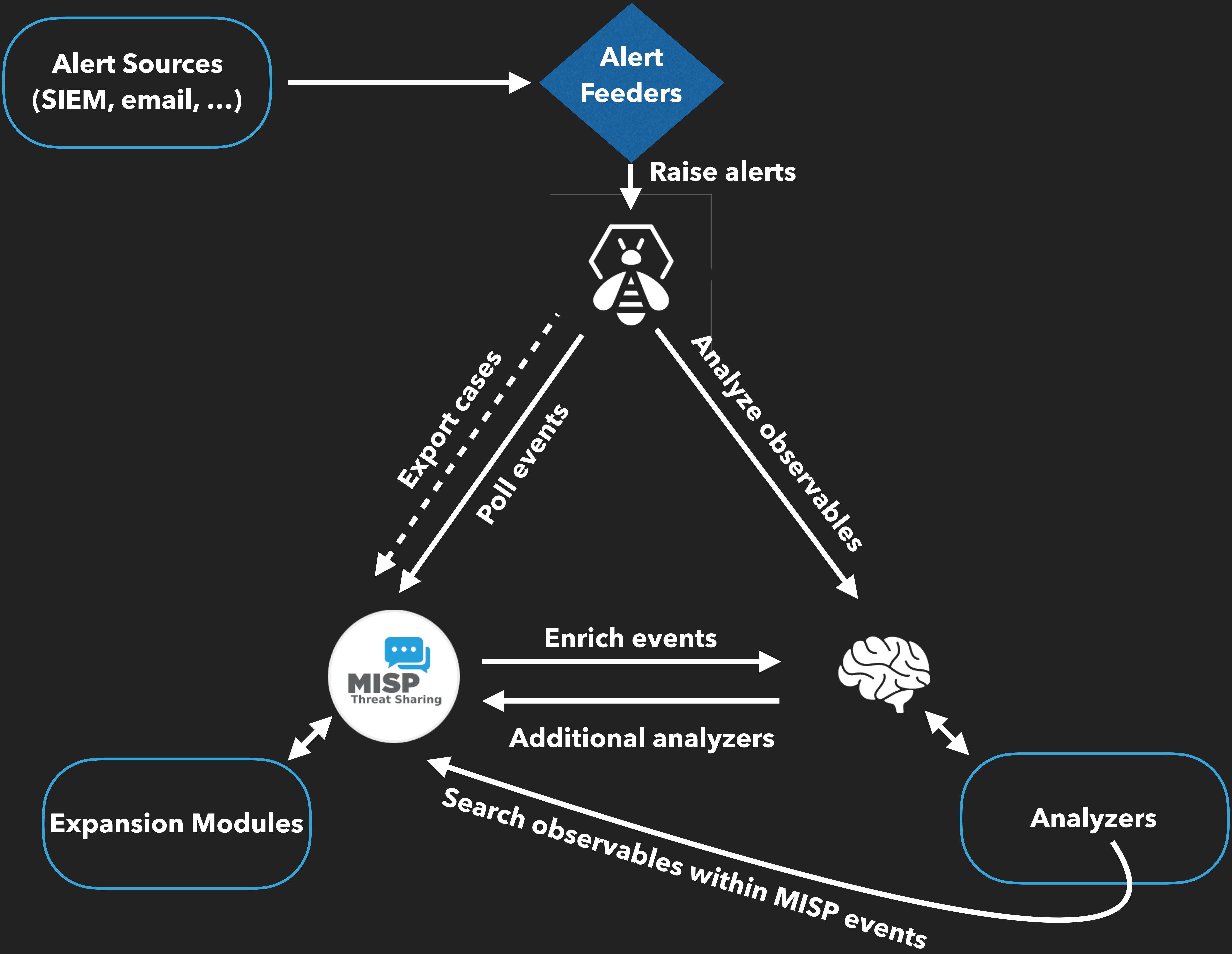
Status
Success

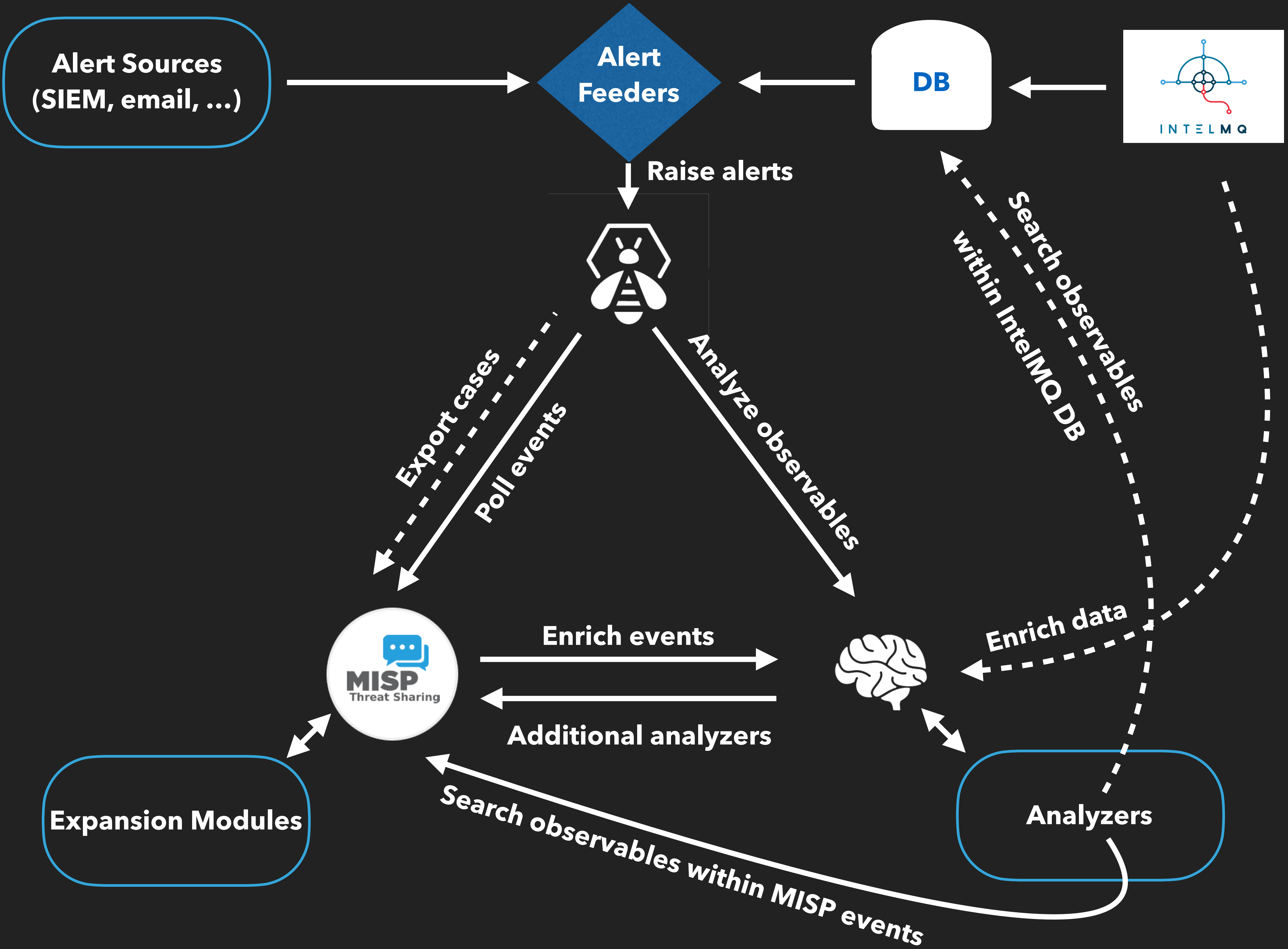
Job report

```
{
  "artifacts": [
    {
      "data": "aefe7efa7236c6ef63d4a970f3756de4d32049dc",
      "attributes": {
        "dataType": "hash"
      }
    },
    {
      "data": "2e8dc58a36806e13cd61e4a25f38c9ee",
      "attributes": {
        "dataType": "hash"
      }
    },
    {
      "data": "https://www.virustotal.com/file/8b3b8fba04773b40d9639ff57755c7f96d8359b23927d0f72654f81
      "attributes": {
        "dataType": "url"
      }
    },
    {
      "data": "8b3b8fba04773b40d9639ff57755c7f96d8359b23927d0f72654f81db671c67d",
      "attributes": {
        "dataType": "hash"
      }
    },
    {
      "data": "2e8dc58a36806e13cd61e4a25f38c9ee",
      "attributes": {
        "dataType": "hash"
      }
    },
    {
      "data": "1.3.0.8876",
      "attributes": {
        "dataType": "ip"
      }
    },
```

PLEASE REWIND

THE BIG PICTURE


Alert Sources
(SIEM, email, …)
Alert
Feeders
Raise alerts
Export cases
Poll events
Analyze observables
MISP
Threat Sharing
Enrich events
Additional analyzers
Expansion Modules
Analyzers
Search observables within MISP events


Alert Sources (SIEM, email, ...)
Alert Feeders
DB
INTELMQ
Raise alerts
Export cases
Poll events
Analyze observables
Search observables within IntelMQ DB
MISP Threat Sharing
Enrich events
Additional analyzers
Enrich data
Expansion Modules
Analyzers
Search observables within MISP events

GET THE SOFTWARE

HTTPS://THEHIVE-PROJECT.ORG/

- TheHive and Cortex are available under an AGPL license
- Use RPM, DEB, Docker image, binary package or build the the source code
- Linux with JRE 8+, Chrome, Firefox, IE (11)
- Test/training VM: https://blog.thehive-project.org/2017/07/06/train-till-you-drain-thehive-cortex-vm/

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
- LDO-CERT
- MEHDI ASCHY
- ANTOINE BRODIN
- GUILLAUME ROUSSE
- MILES NEFF