TheHive

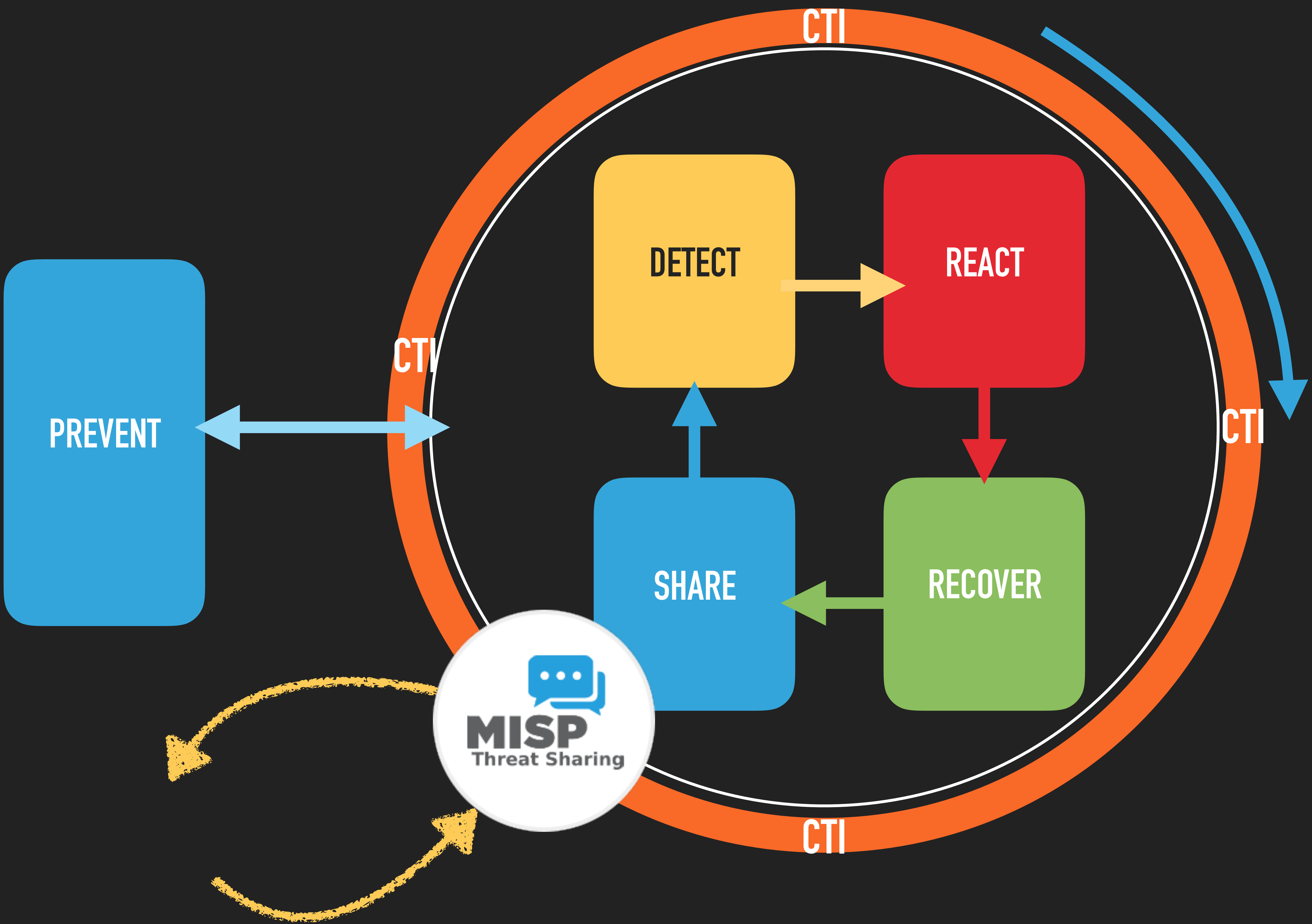
MISP SUMMIT 3 / 2017-10-16

TLP:WHITE

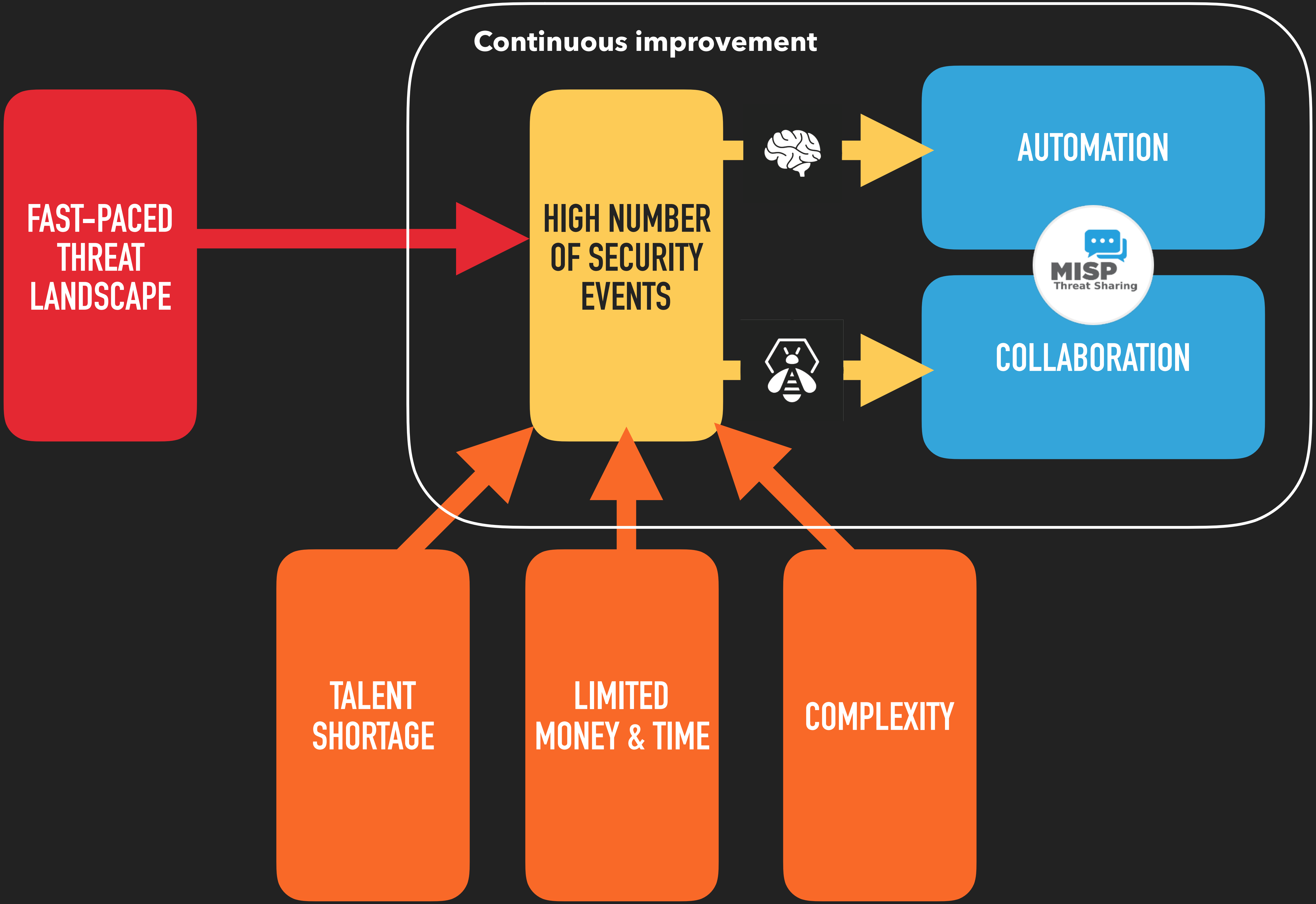
FROM CTI TO DFIR & BACK
WITH MISP, THEHIVE & CORTEX

Saâd Kadhi
TheHive Project Leader

WHEN PREVENTION FAILS



DRIVE DOWN THE TIME TO REACT

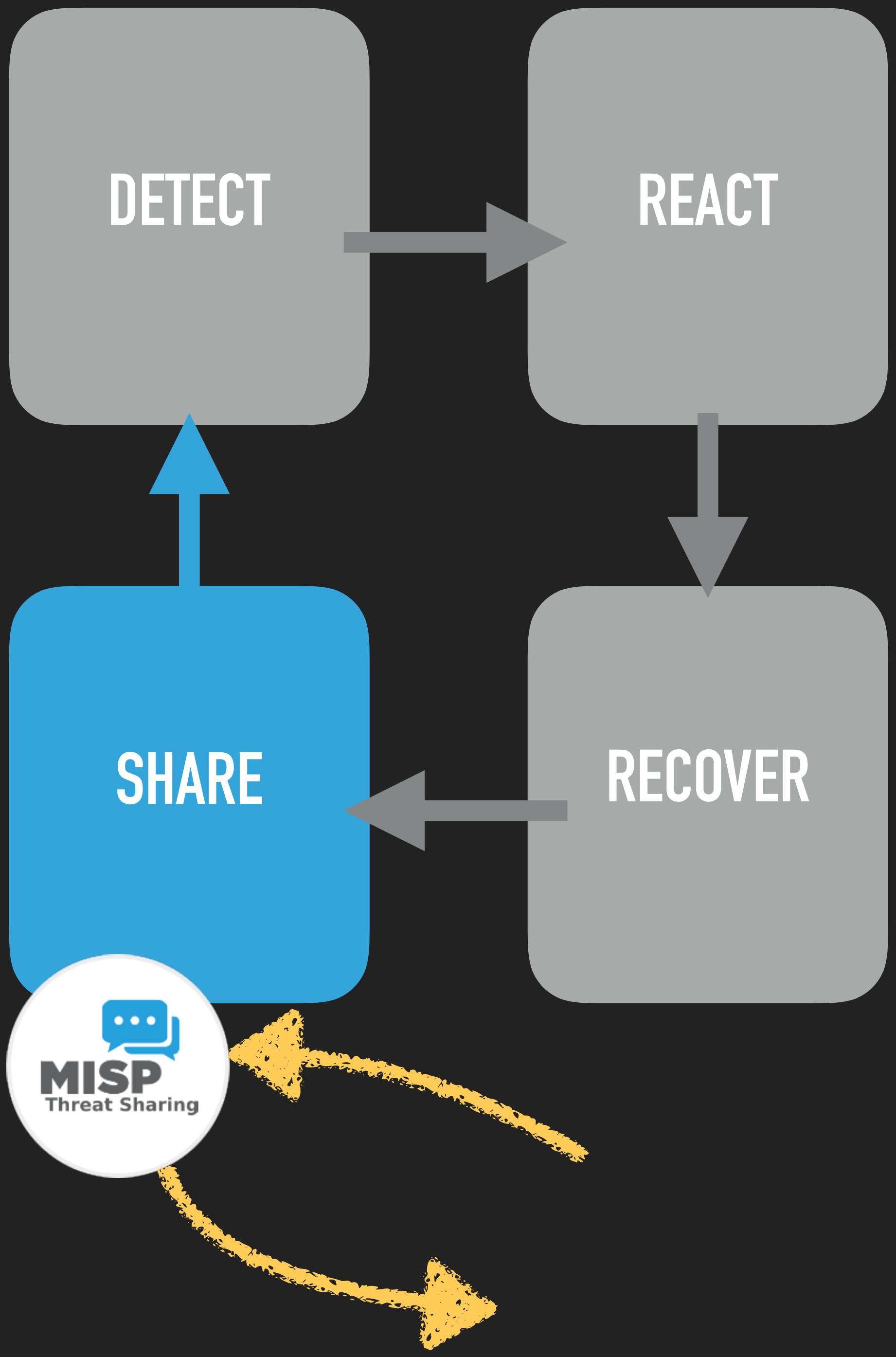


FACTS

- Threat Intelligence, Digital Forensics, Incident Response = team work
- We shall seek to drive these activities and continuously improve them
- Thanks to operational, meaningful statistics

SHARING IS CARING / MY DETECTION IS YOUR PREVENTION / …

- Investigation performed, IOCs collected and proper response done
- Is it time to rest? No
- Some if not all IOCs should be shared
- They might prove useful to peers for defending themselves
- Hopefully, they will come up with complementary IOCs that were unbeknownst to us



LEARNING FROM BEES

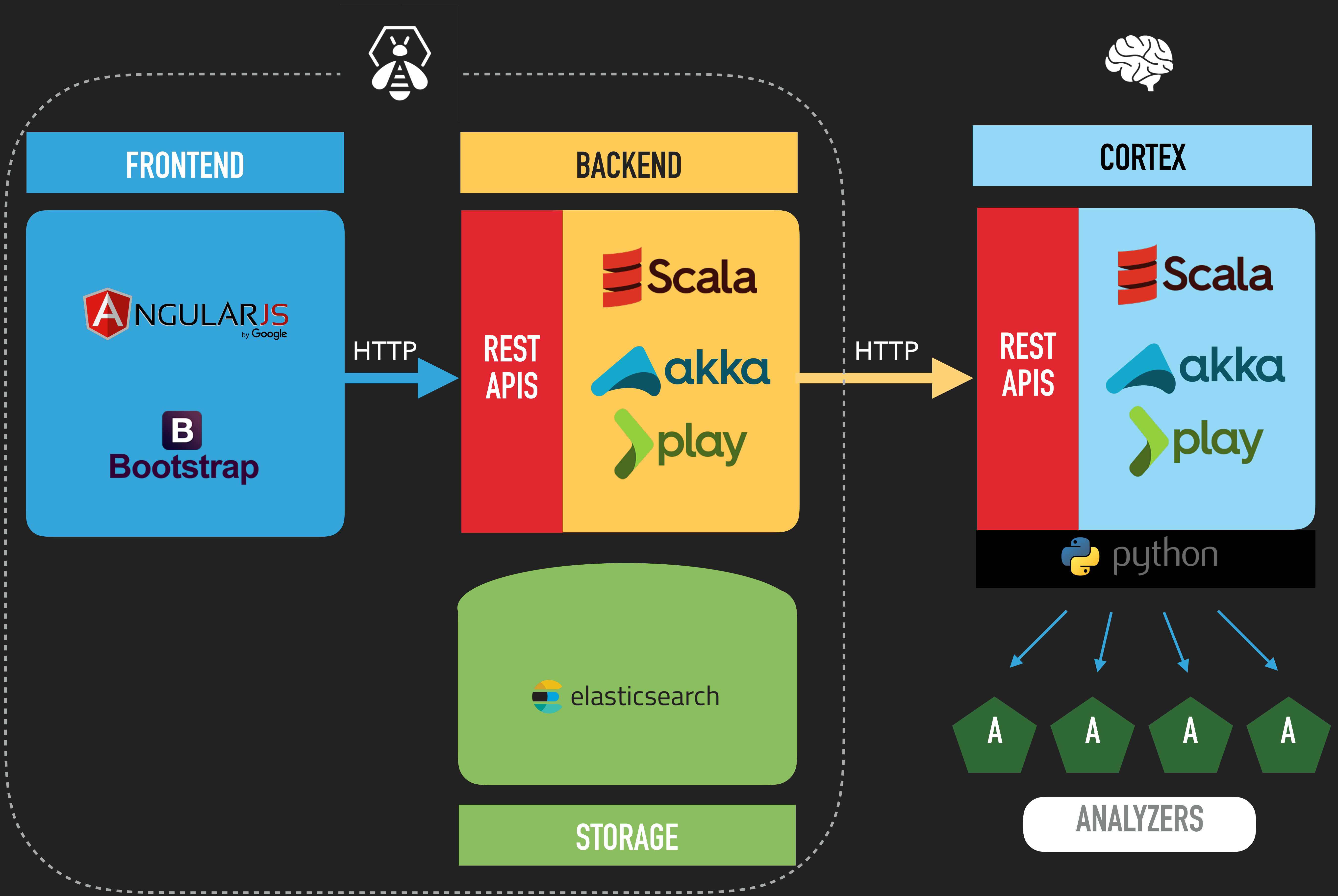
- Security Incident Response Platform (SIRP)
  - Collaboration
  - Task & work log
  - Analysis and IOC storage
- Authentication: LDAP, Active Directory, API keys & local accounts
- Used by several cybersecurity teams throughout the world

Cortex

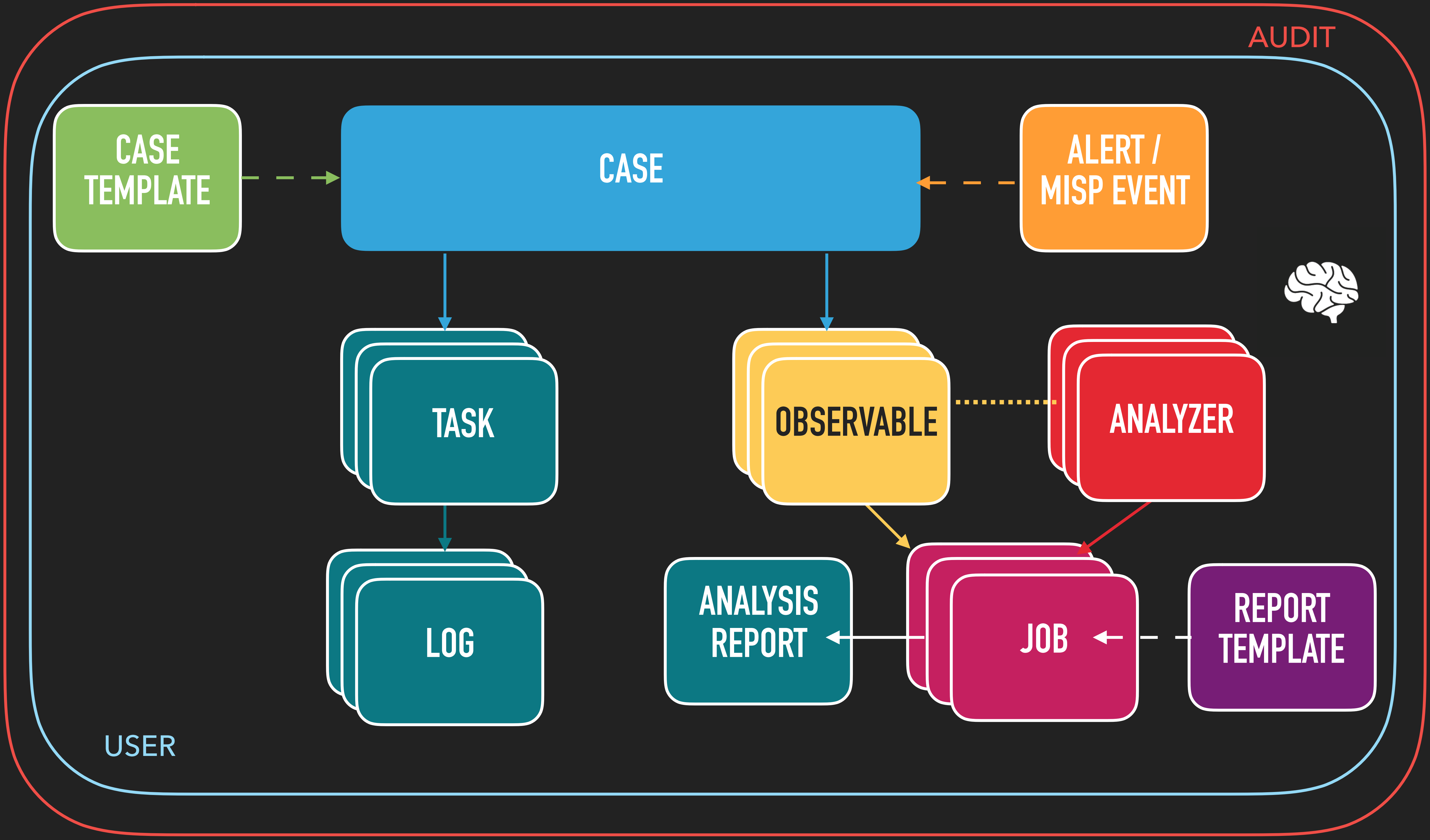
MADE IN FRANCE

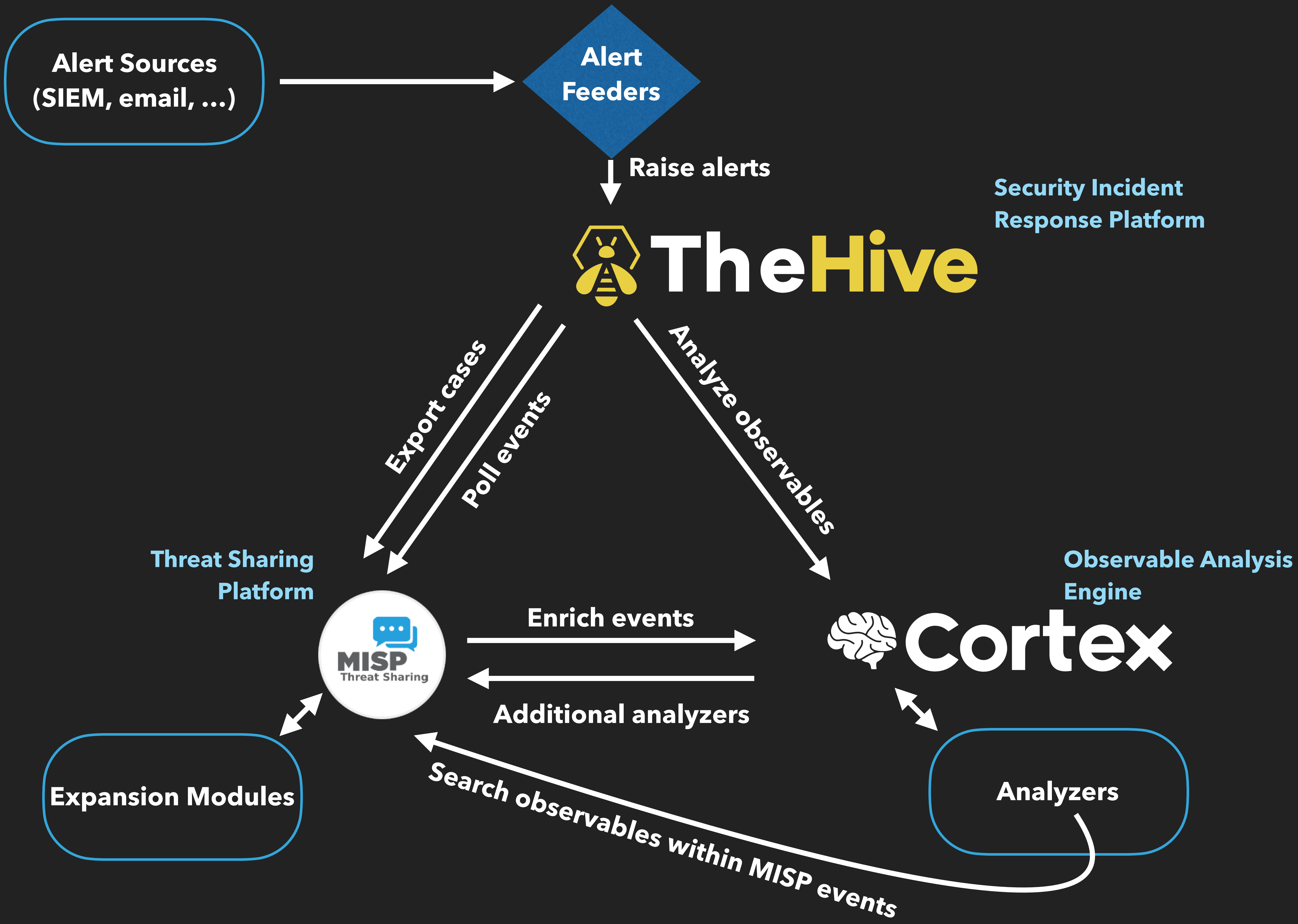
- Query analyzers through a Web UI to quickly assess the malicious nature of observables
- Automate bulk observable analysis
- Analyzers can be developed in any programming language that is supported by Linux
- Invoke MISP expansion modules
- Can be queried from MISP to enrich events

ARCHITECTURE



WORKFLOW


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



Alert Sources (SIEM, email, ...)

Alert Feeders

Raise alerts

TheHive

Security Incident Response Platform

Export cases

Poll events

Analyze observables

Threat Sharing Platform

MISP Threat Sharing

Enrich events

Additional analyzers

Observable Analysis Engine

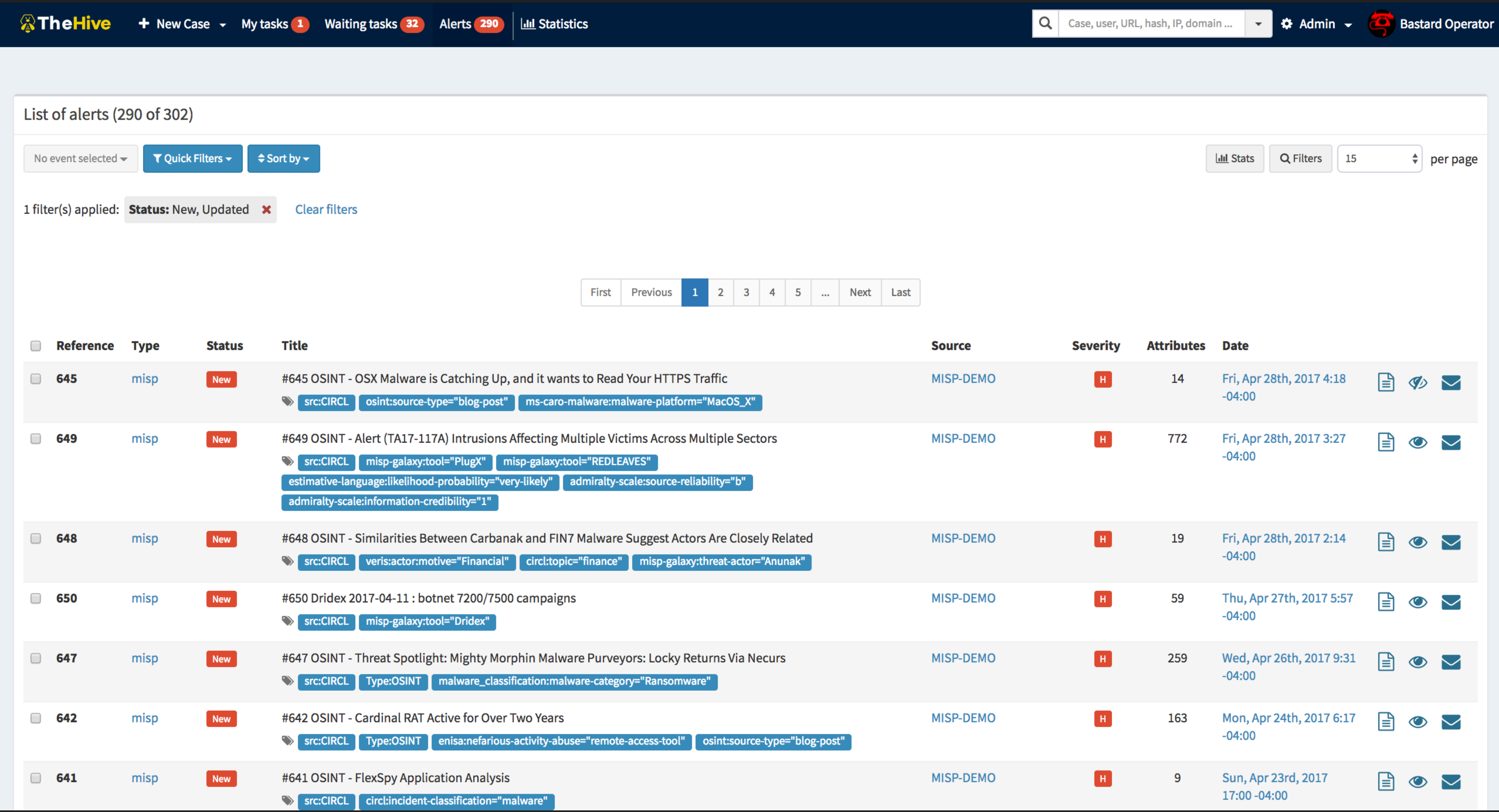
Cortex

Expansion Modules

Analyzers

Search observables within MISP events

ALERT PANEL

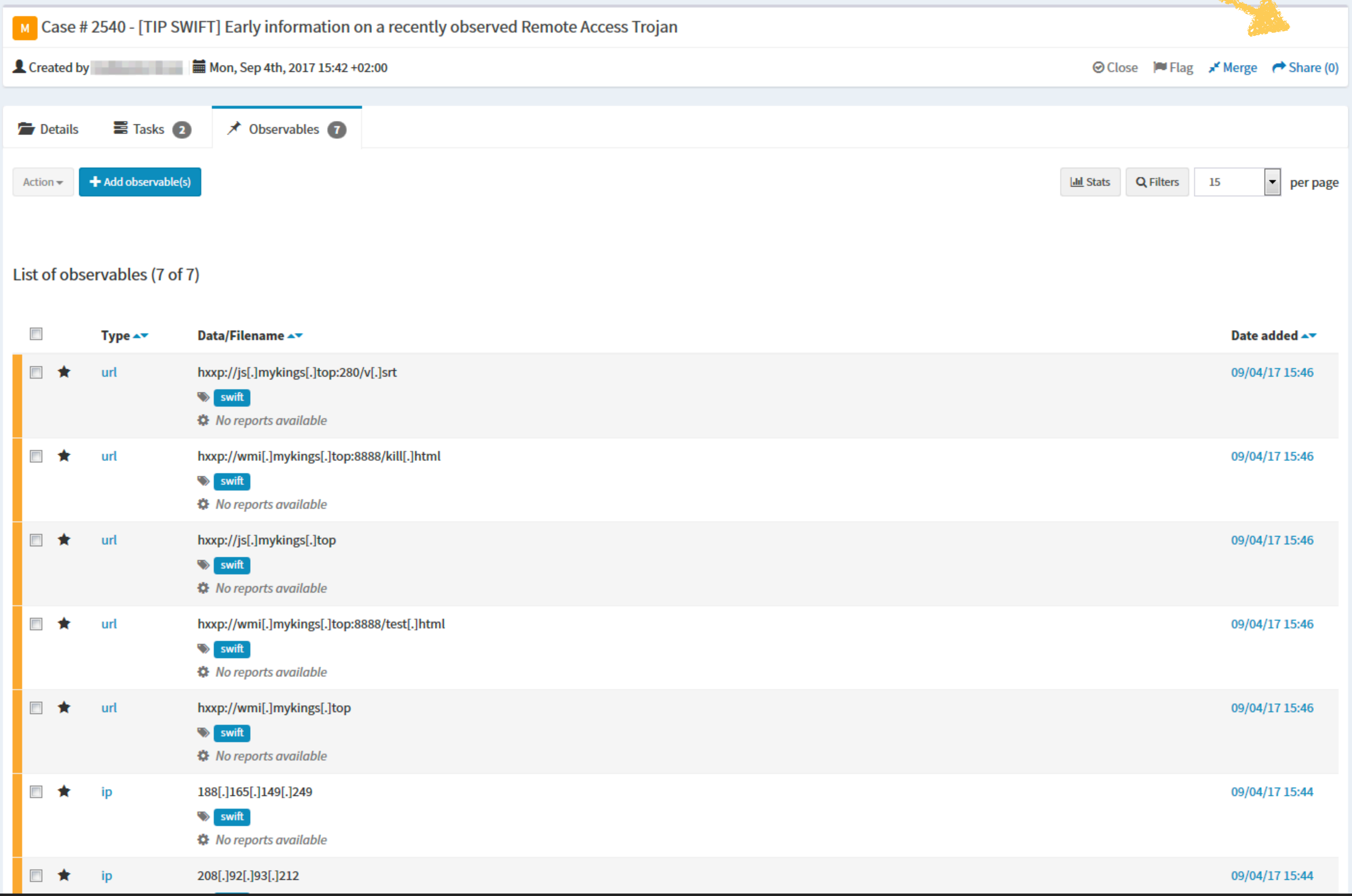


List of alerts (290 of 302)

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

EXPORT CASE



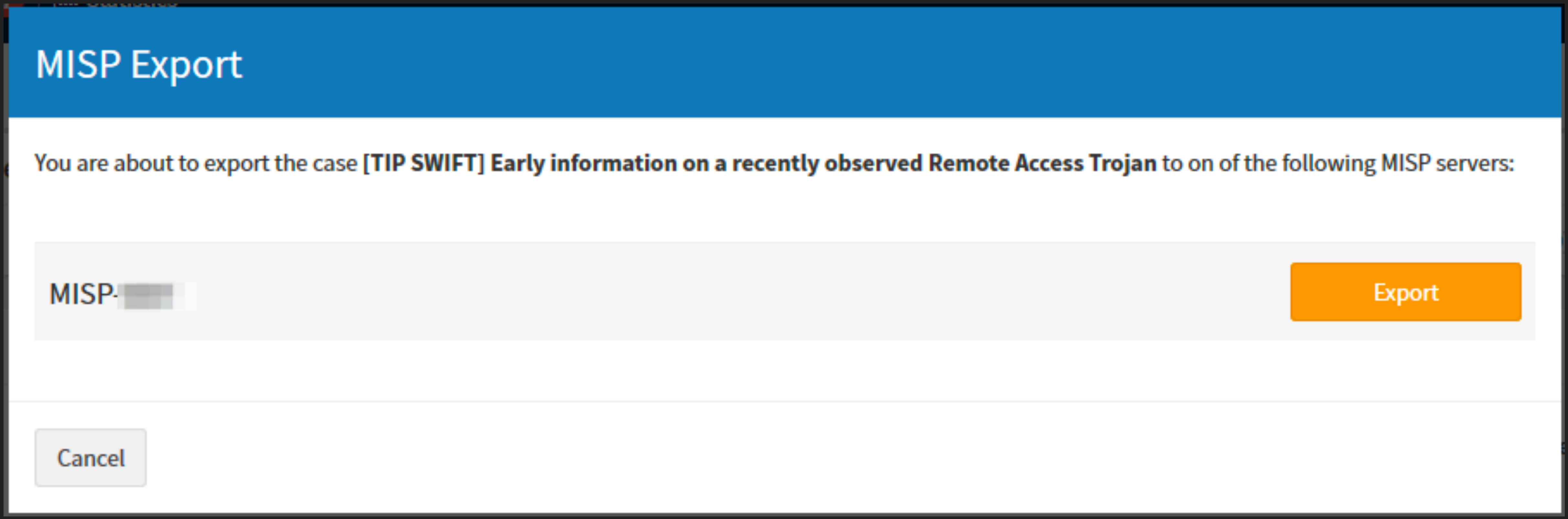
M Case # 2540 - [TIP SWIFT] Early information on a recently observed Remote Access Trojan

Created by [redacted] Mon, Sep 4th, 2017 15:42 +02:00

List of observables (7 of 7)

□		Type	Data/Filename	Date added
□	★	url	hxxp://js[.]mykings[.]top:280/v[.]srt swift *No reports available*	09/04/17 15:46
□	★	url	hxxp://wmi[.]mykings[.]top:8888/kill[.]html swift *No reports available*	09/04/17 15:46
□	★	url	hxxp://js[.]mykings[.]top swift *No reports available*	09/04/17 15:46
□	★	url	hxxp://wmi[.]mykings[.]top:8888/test[.]html swift *No reports available*	09/04/17 15:46
□	★	url	hxxp://wmi[.]mykings[.]top swift *No reports available*	09/04/17 15:46
□	★	ip	188[.]165[.]149[.]249 swift *No reports available*	09/04/17 15:44
□	★	ip	208[.]92[.]93[.]212	09/04/17 15:44

EXPORT CASE

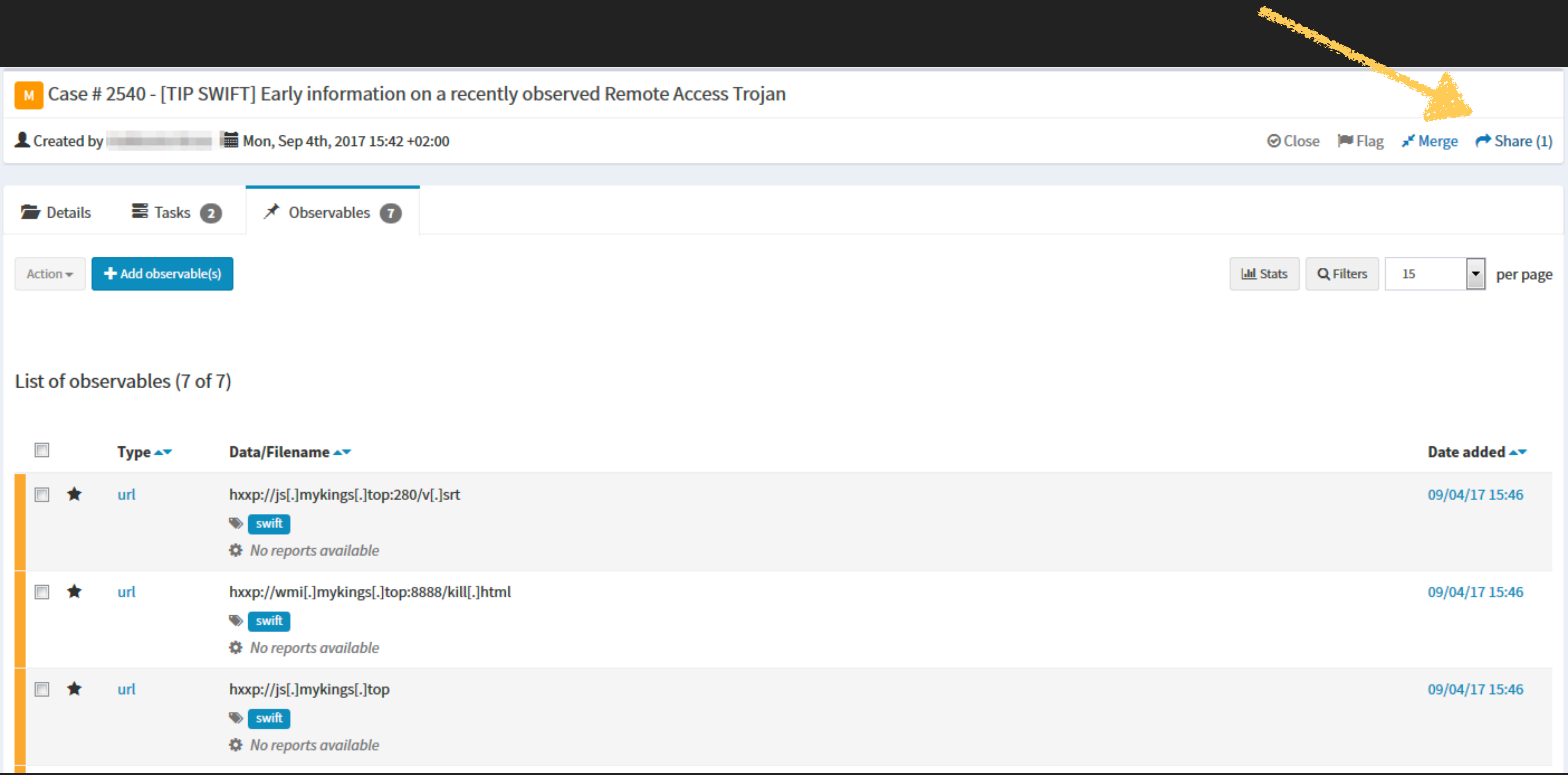


MISP Export

You are about to export the case **[TIP SWIFT] Early information on a recently observed Remote Access Trojan** to on of the following MISP servers:

MISP-[redacted]

EXPORT CASE



M Case # 2540 - [TIP SWIFT] Early information on a recently observed Remote Access Trojan

Created by [redacted] Mon, Sep 4th, 2017 15:42 +02:00

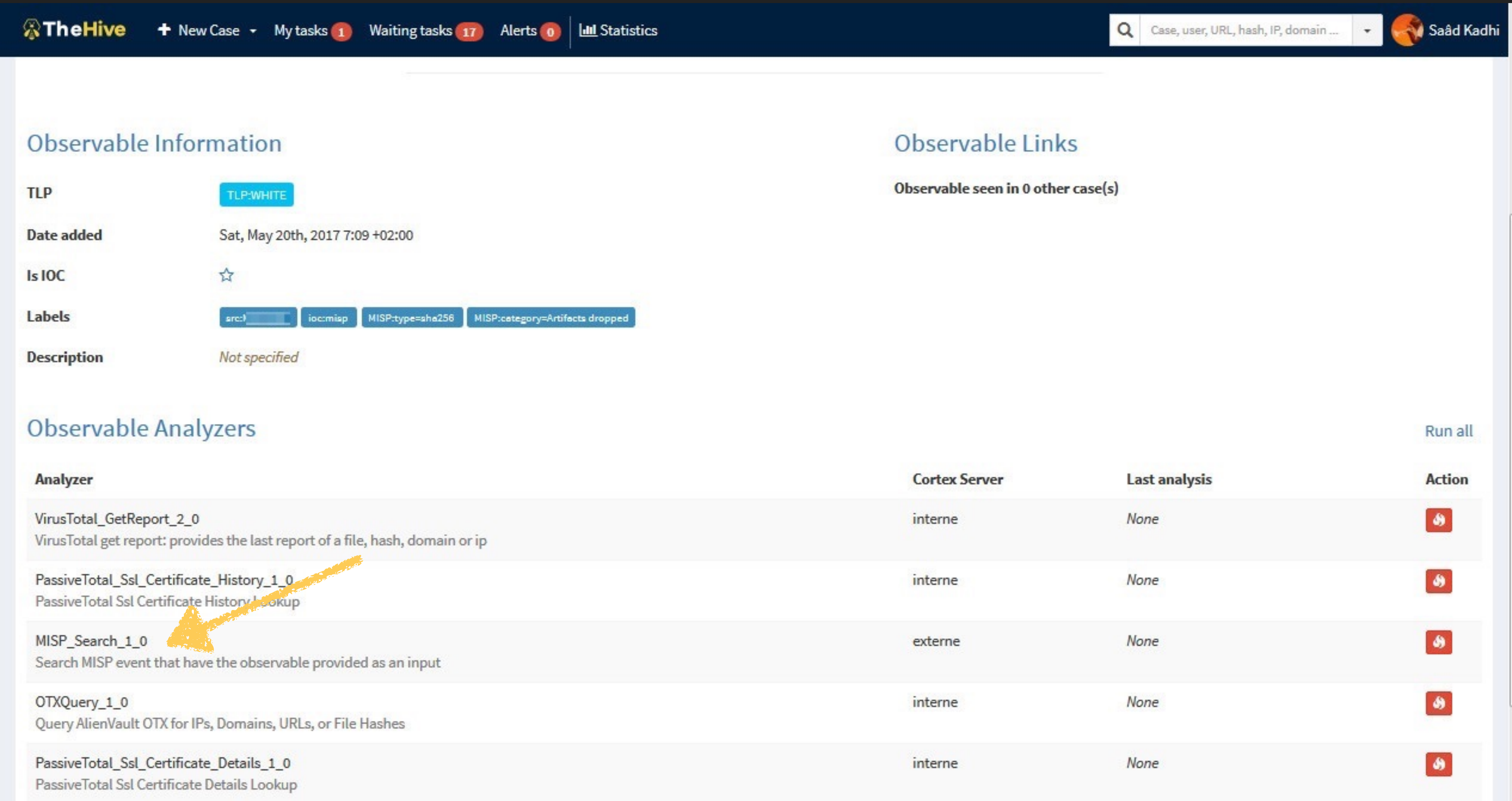
List of observables (7 of 7)

		Type	Data/Filename	Date added
□	★	url	hxxp://js[.]mykings[.]top:280/v[.]srt swift *No reports available*	09/04/17 15:46
□	★	url	hxxp://wmi[.]mykings[.]top:8888/kill[.]html swift *No reports available*	09/04/17 15:46
□	★	url	hxxp://js[.]mykings[.]top swift *No reports available*	09/04/17 15:46

27 ANALYZERS (AND COUNTING)

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

ANALYSIS EXAMPLE



Observable Information

TLP: TLP:WHITE

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

Is IOC: ☆

Labels: src:[redacted] ioc:misp MISP:type=sha256 MISP:category=Artifacts dropped

Description: *Not specified*

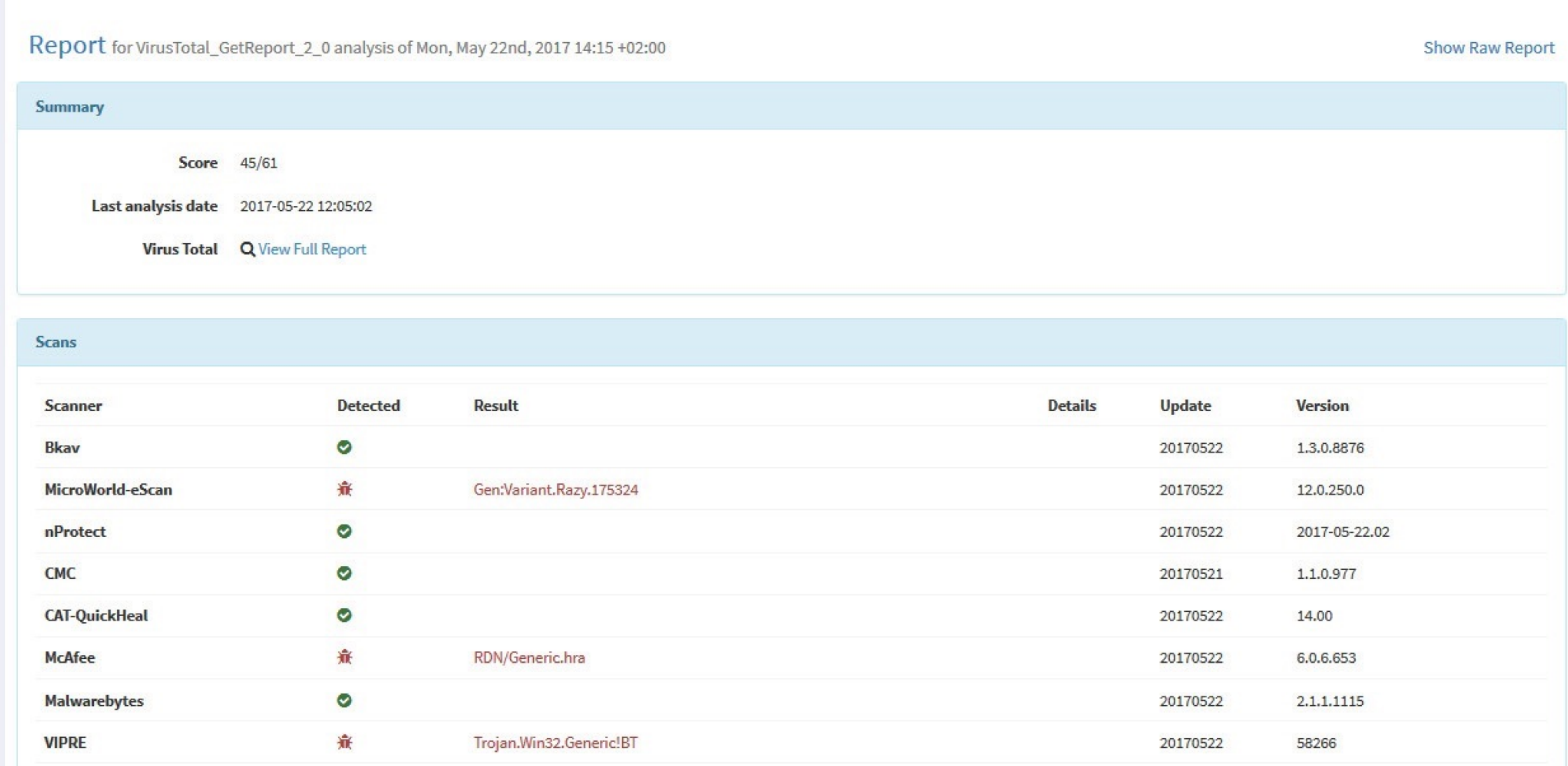
Observable Links

Observable seen in 0 other case(s)

Observable Analyzers

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*	

ANALYSIS EXAMPLE



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

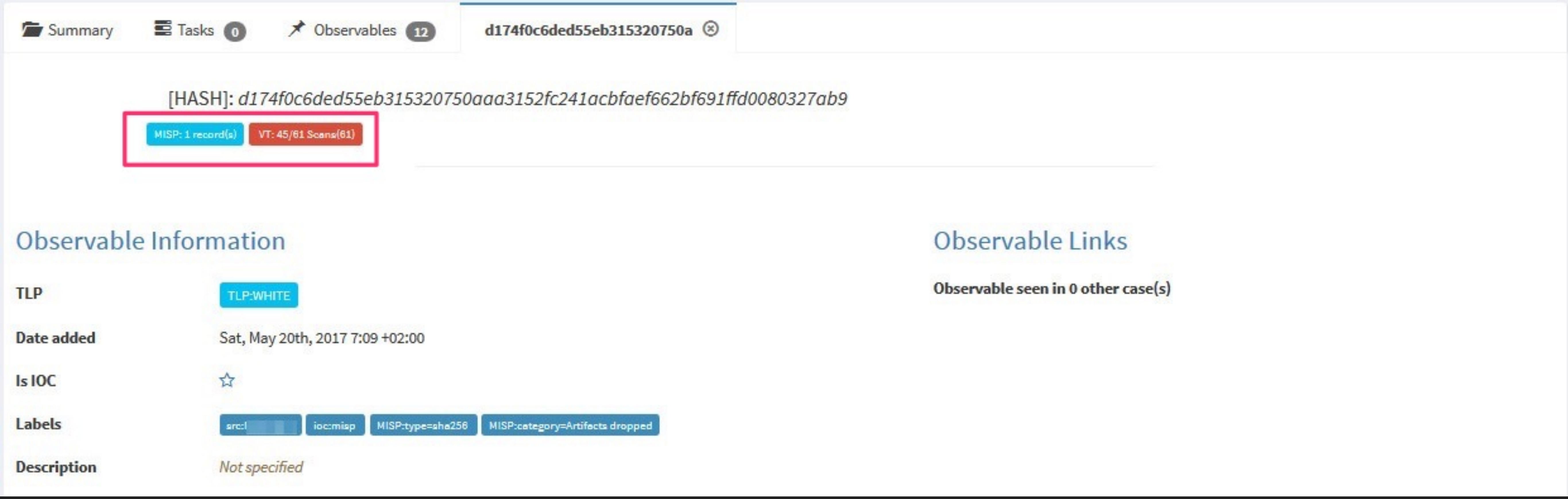
Summary

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

ANALYSIS EXAMPLE



[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:[redacted] ioc:misp MISP:type=sha256 MISP:category=Artifacts dropped
Description	*Not specified*

Observable Links

Observable seen in 0 other case(s)

THEHIVE — RECAP

- Import from and export to multiple MISP instances
- Preview alerts from multiple sources (SIEM, IDS, email…)
- Analyze observables through several Cortex instances
- Leverage statistics to drive the activity
- Use webhooks to open tickets in IT ticketing systems
- Work as a team thanks to the real-time stream

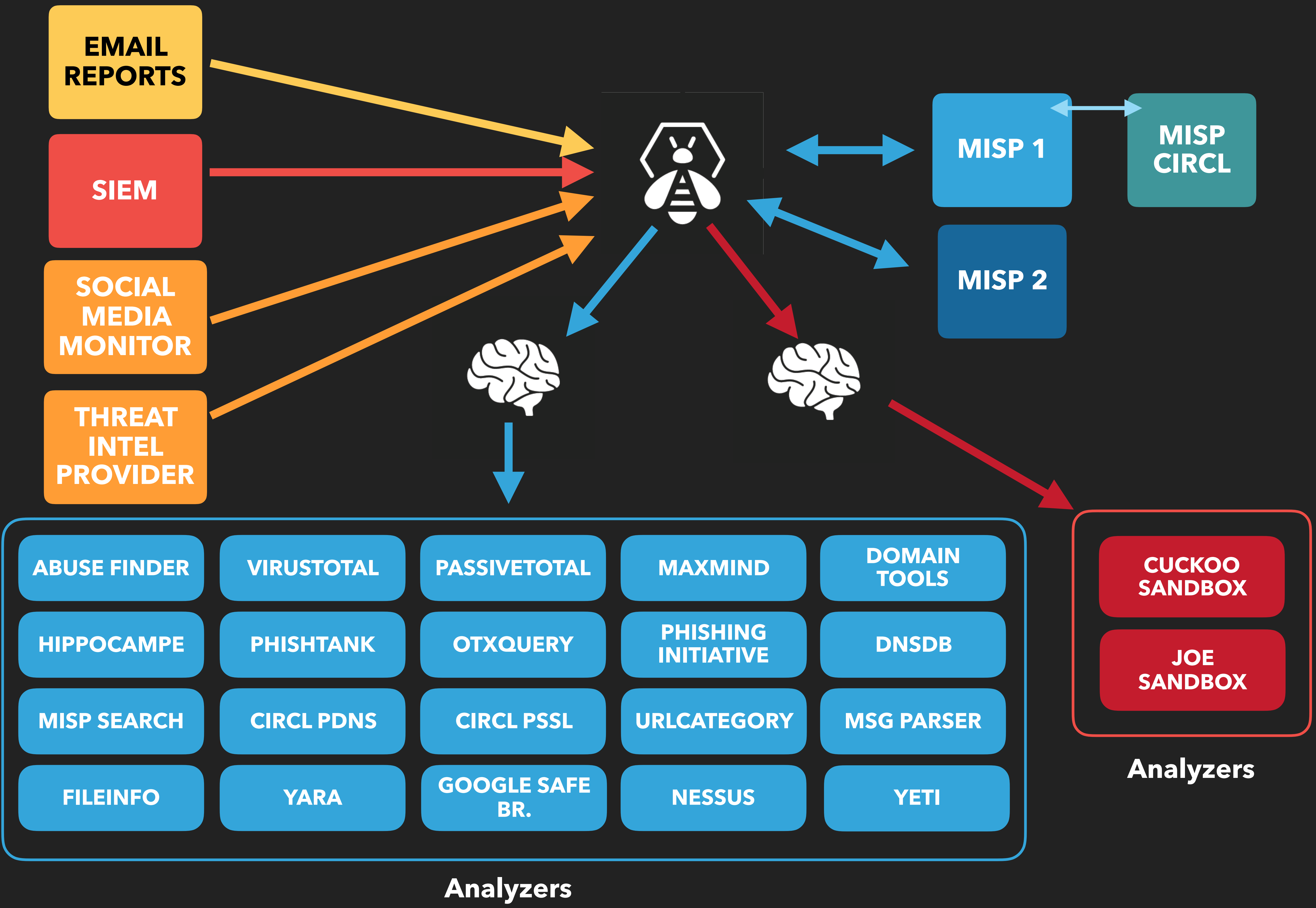
ADDITIONAL SOFTWARE

- TheHive4Py - Python lib to create alert/case from multiple sources
- Splunk App - create alerts out of Splunk. dev. by Miles Neff
- Elastalert Hive Alerter - use a custom Elastalert Alert to create alerts. contributed by Nclose
- Cortex4py - Python lib to submit observables in bulk mode through the Cortex REST API from alternative SIRP platforms & custom scripts

USE IT

S

USE CASE



EMAIL REPORTS

SIEM

SOCIAL MEDIA MONITOR

THREAT INTEL PROVIDER

MISP 1

MISP CIRCL

MISP 2

ABUSE FINDER

VIRUSTOTAL

PASSIVETOTAL

MAXMIND

DOMAIN TOOLS

HIPPOCAMPE

PHISHTANK

OTXQUERY

PHISHING INITIATIVE

DNSDB

MISP SEARCH

CIRCL PDNS

CIRCL PSSL

URLCATEGORY

MSG PARSER

FILEINFO

YARA

GOOGLE SAFE BR.

NESSUS

YETI

Analyzers

CUCKOO SANDBOX

JOE SANDBOX

Analyzers

GET THE SOFTWARE

TRAINING VM AVAILABLE

- TheHive, Cortex and MISP are available under a, free, open source AGPL license
- TheHive and Cortex can be installed using RPM, DEB, Docker image, binary package or built from the source code
- Linux with JRE 8+, Chrome, Firefox, IE (11), and a decent computer
- https://thehive-project.org/
- https://misp-project.org/

QUESTIONS?

THEHIVE PROJECT

CORE TEAM

NABIL ADOUANI

THOMAS FRANCO

SAÂD KADHI

JÉRÔME LEONARD

CONTRIBUTORS

CERT-BDF

CERT-BUND

RÉMI POINTEL

MILES NEFF

ERIC CAPUANO

MEHDI ASCHY

ANTOINE BRODIN

GUILLAUME ROUSSE

NICK PRATLEY