



THE BEST PARTNER IN CRIME OF YOUR SIEM

Nabil Adouani

---

Co-founder of **TheHive Project**  
CEO of **StrangeBee**  
@TheHive\_Project | @StrangeBeeInc

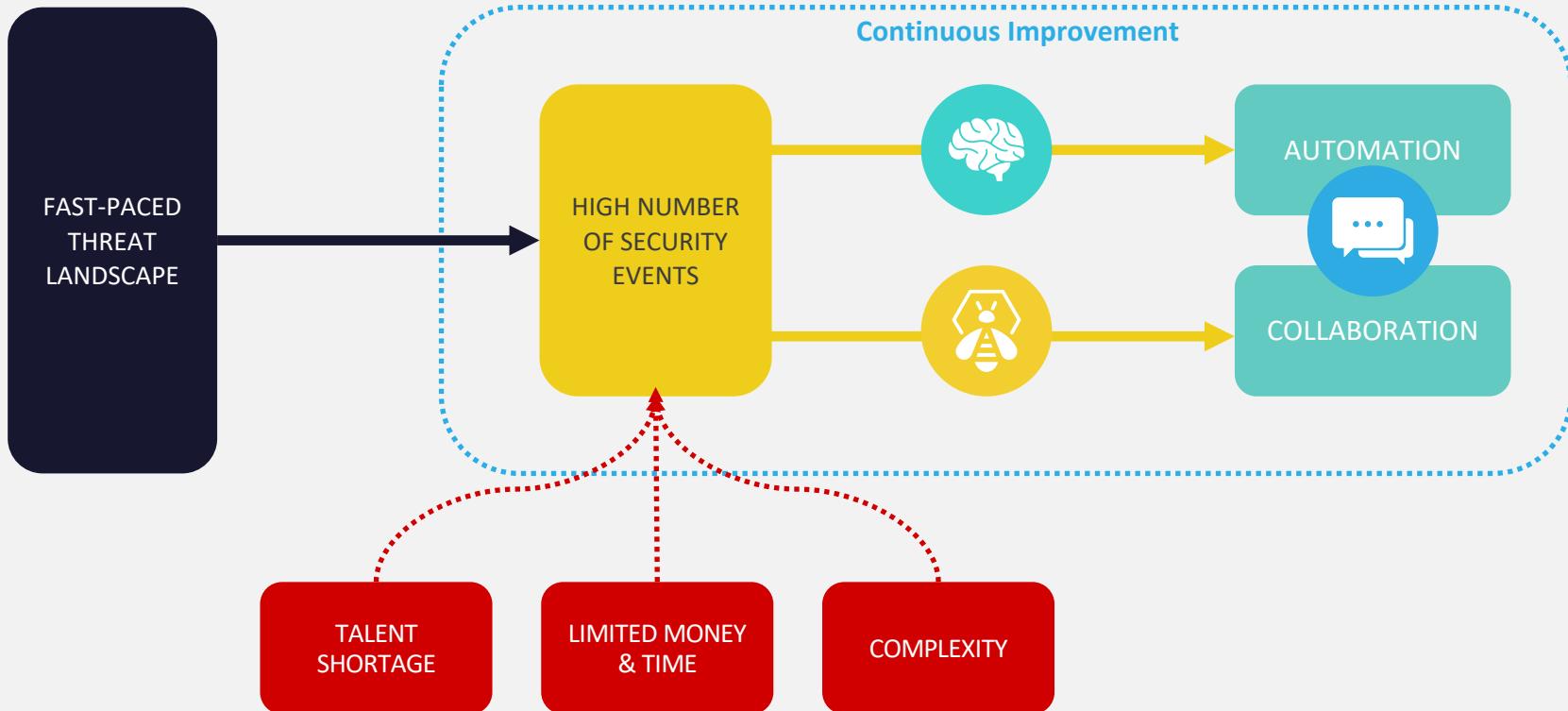


# The Agenda

---

- Story & purpose
- Overview: terminology and how it works
- TheHive and SIEMs
- IR using TheHive & Cortex
- Features
- Q&A

# Drive Down The Time to React



# The Products



## Security Incident Response

TheHive - + New Case | My tasks (0) | Waiting tasks (21) | Alerts (1) | Dashboards | Search

Case # 69 - [MALSPAM]Avis Business Club: Booking Confirmation

Jerome Leonard 05/26/20 15:12 0 21 days 2 cases 1 alert

Sharing (1) | Close Unflag Merge Remove | Export (0) | Responders

Details Tasks Observables doc\_0780ca66fcfed4250ab5ac23e976e970a

Action + Add observable Export

IM Stats Filters 15 per page

### Observable List (3 of 6)

1 filter(s) applied: dataType:file,ip Clear filters

Type	Value/Filename	Date Added	Actions
ip	209.85.122.165	05/26/20 15:18	[file] doc_0780ca66fcfed4250ab5ac23e976e970a
file	[Avis Business Club] Booking Confirmation Email[.]eml	05/26/20 15:12	[file] doc_0780ca66fcfed4250ab5ac23e976e970a
file	doc_0780ca66fcfed4250ab5ac23e976e970a	05/26/20 15:12	[file] doc_0780ca66fcfed4250ab5ac23e976e970a

## Observable Analysis and Active Response

Cortex - + New Analysis

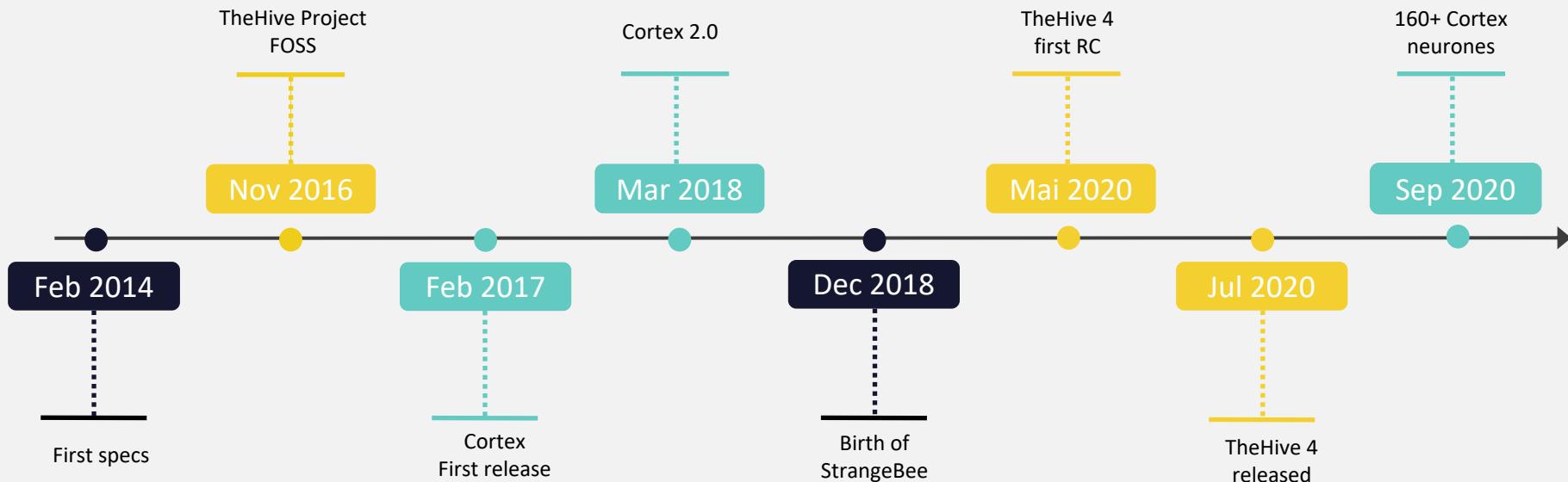
Jobs History (78)

Data Types (9) Job Type (2) Analyzers (17) Observable

Select analyzer 5 selected Search Clear Pagination 1 2 3 4 50 / page

Status	Job details	TLP	PAP
Success	[file] doc_0780ca66fcfed4250ab5ac23e976e970a Analyzer: ThreatGrid_1_0 Date: an hour ago User: cert/thehive TLP:AMBER PAP:AMBER		
Success	[file] doc_0780ca66fcfed4250ab5ac23e976e970a Analyzer: FileInfo_7_0 Date: an hour ago User: cert/thehive TLP:AMBER PAP:AMBER		
Success	[hash] 2A244721FF221172EDB788715D11008F0AB50AD946592F355BA16CE97A23E055 Analyzer: ThreatResponse_1_0 Date: an hour ago User: cert/thehive TLP:GREEN PAP:AMBER		
Success	[hash] 1569F6FD28C666241902A19B205E8223D47CCDD08C92FC35E867C487EBC999 Analyzer: ThreatResponse_1_0 Date: an hour ago User: cert/thehive TLP:GREEN PAP:AMBER		
Success	[hash] 87AACD95A8C9740F14B401BD6D7CC5CE2E2B9BECC750F32D1D9C858BC101DFFA Analyzer: ThreatResponse_1_0 Date: an hour ago User: cert/thehive TLP:GREEN PAP:AMBER		
Success	[domain] centredairenantes[.]fr		

# The Timeline





# TheHive & Cortex Overview

# TheHive overview



## Security Incident Response Platform

The screenshot shows a TheHive interface for a security incident. The top navigation bar includes links for 'New Case', 'My tasks', 'Waiting tasks', 'Alerts', 'Dashboards', and 'Search'. The main title is 'Case # 69 - [MALSPAM]Avis Business Club: Booking Confirmation'. Below the title, it shows 'Sharing (1)', 'Close', 'Unflag', 'Merge', 'Remove', 'Export (0)', and 'Responders'. The main content area displays an 'Observable List (3 of 6)' with a single filter applied: 'datatype:file, ip'. The list contains three items:

Type	Value/Filename	Date Added	Actions
ip	209[.]85[.]220[.]65 ↳ action, add to blacklist   Mailservers.Request for blacklisting   src.EmailParser_1_3   src.suspicious_email   remote smtp server ↳ VT.GetReport="0 detected url(s)"   Oxygene.DNS Forwarder->forwarder-mail-user.firebaseio.com.last_seen:2020-05-06"   DShield.Score="0 count(s) / 0 attack(s) / 0 threatfeed(s)" ↳ TR-Talos Intelligence="Clean"	05/26/20 15:18	[dropdown]
file	[Avis Business Club] Booking Confirmation Email_[jeml] ↳ None ↳ EmailParser.Attachments="1"	05/26/20 15:12	[dropdown]
file	doc_0780ca66fced4250ab5ac23e976e970a ↳ None ↳ VT.GetReport="4/5/1"   FileInfo.Derivative="Hex string"   FileInfo.FileType="DOC"   FileInfo.Derivative="Base64 string"   FileInfo.DOE="None"   TG.Analysis="10%"	05/26/20 15:12	[dropdown]

- **Organize**, structure and archive incidents including technical artifacts
- **Aggregate**, collect and **triage** Alert
- **Manage** Cases and Tasks
- **Enrich** IOCs and Observables
- **Implement** IR workflows and **playbooks**
- **Take care of information classification levels** (TLP & PAP)
- **Collaborative** & multi tenant platform
- Built-in integration with Cortex for **Analysis** and **Active Response**
- Built-in integration with Threat Intelligence Sharing platform (MISP)

# Cortex overview

- Define libraries of analyzers and responders (3<sup>rd</sup> party connectors)
- Analyze Observables/IOCs from TheHive to gather Intelligence and information
- Run automatic actions on the network to speed up Incident Response
- Take care of information classification levels (TLP & PAP)
- Customize jobs and reports caching
- Customize analyzer rate limiting
- Allow multi-tenant usage

The screenshot shows the Cortex web application interface. At the top, there's a navigation bar with the Cortex logo, a search bar, and links for 'Jobs History', 'Analyzers', 'Responders', 'Organization', and a user account. Below the navigation is a section titled 'Observable Analysis and Active Response Platform'. The main content area is titled 'Jobs History (78)'. It features a table with columns for 'Status', 'Job details', 'TLP', and 'PAP'. Each row represents a job entry with details like file or hash types, analyzer names, dates, users, and classification levels (e.g., TLP:AMBER, PAP:AMBER). There are also 'View' and 'Delete' buttons for each entry.

Status	Job details	TLP	PAP
Success	[file] doc_0780ca66fcfed4250ab5ac23e976e970a Analyzer: ThreatGrid_1_0 Date: an hour ago User: cert/thehive	TLP:AMBER	PAP:AMBER
Success	[file] doc_0780ca66fcfed4250ab5ac23e976e970a Analyzer: Fileinfo_7_0 Date: an hour ago User: cert/thehive	TLP:AMBER	PAP:AMBER
Success	[hash] 2A44721FF221172EDB788715D11008F0AB50AD946592F355BA16CE97A23E055 Analyzer: ThreatResponse_1_0 Date: an hour ago User: cert/thehive	TLP:GREEN	PAP:AMBER
Success	[hash] 1569F6D28C666241902A19B205EE8223D47CCDD08C92FC35E867C487EBC999 Analyzer: ThreatResponse_1_0 Date: an hour ago User: cert/thehive	TLP:GREEN	PAP:AMBER
Success	[hash] 87AAC95A8C9740F14B401BD6D7CC5CE2E2B9BECC750F32D1D9C858BC101DFFA Analyzer: ThreatResponse_1_0 Date: an hour ago User: cert/thehive	TLP:GREEN	PAP:AMBER
Success	[domain] centredentairenantes[.]fr	TLP:GREEN	PAP:AMBER

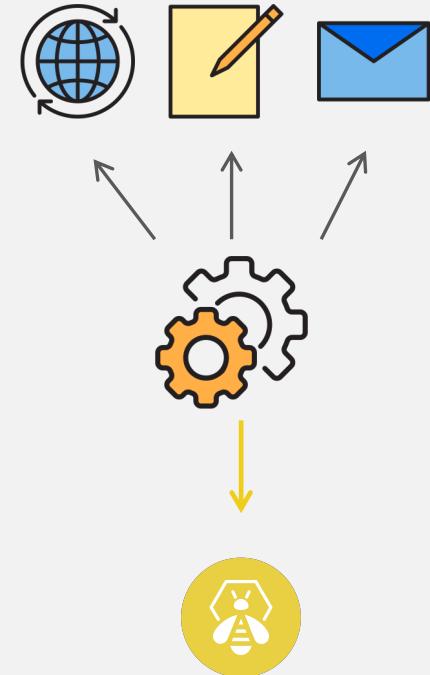
# Terminology

## Feeders, Analyzers and Responders

# Feeders

---

- **Gather** information from an **external service**
  - Mail server, CTI provider, SIEM, EDR, NDR...
  - Ticketing system...
- **Process** data and **format** it as TheHive objects
- **Import** data as Case or Alert
- Python Client Library – [TheHive4py](#)



# Feeders

- Example: *Gather reports of suspicious messages received by internal users, and generate Alerts*

Suspicious email

From john@training.strangebee.com 

To csirt@training.strangebee.com 

Date Today 09:30

Message 1 of 2  

Hello,  
please find attached a suspicious email I received.  
Could you please investigate ?  
Best,  
John,

 Invoice\_No\_131315.eml (106 ...)

**Alert Preview** **New**

 **Invoice No. #131315**

 **ID:** 82604136  **Date:** Fri, Jun 26th, 2020 9:32 +02:00  **Type:** email report  **Reference:** 1aa871  **Source:** Internal mail Server

 **suspicious\_email**  **submittedBy:**john@training.strangebee.com

**Description**

Hello,  
please find attached a suspicious email I received. Could you please investigate ?  
Best, John,

**Additional fields**

training:reportedBy	john@training.strangebee.com
---------------------	------------------------------

**Observables (4)**

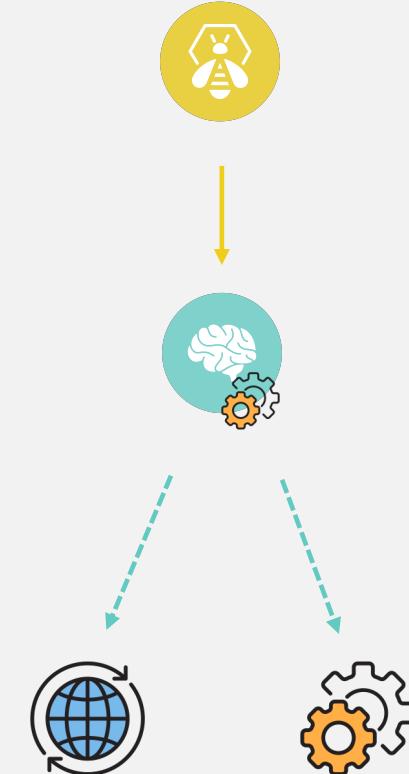
All (4) mail (1) mail-subject (1) file (2)

Type	Data
mail	noreplies@tele[.]fi  <b>suspicious_mail_src_addr</b>
mail-subject	Invoice No[.] #131315  <b>suspicious_mail.mail-subject</b>
file	outstanding-payment-2428.doc (77312 bytes)  <b>suspicious_mail.email_attachment</b>
file	Invoice_No_131315.eml (108328 bytes)  <b>suspicious_mail.email_source</b>

# Analyzers

---

- **Process** one (1) *Observable*
- **Deliver** an analysis report
  - Query external services
  - CTI, IP/Domain repurtation, Sandboxes...
- **Input:** Observable metadata and configuration
- **Output:** Summary report + Long report + Observables (*optional*)



# Analyzers

- Example: Get VirusTotal report from a Hash file

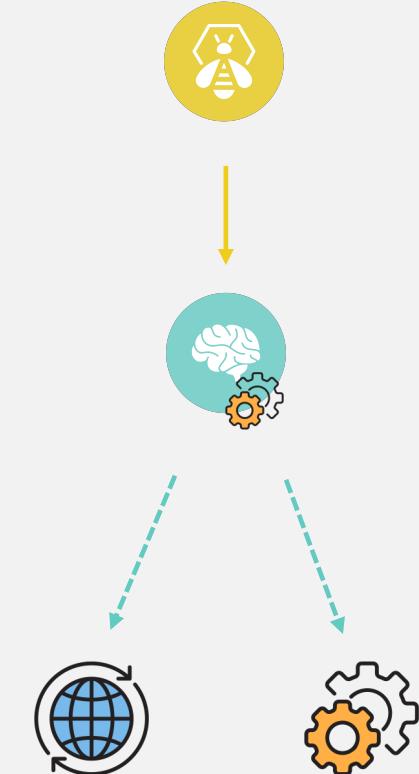
Summary						
Scans						
Scanner	Detected	Result	Details	Update	Version	
Bkav	✓			20200512	1.3.0.9899	
MicroWorld-eScan	✗	Trojan.GenericKD.41432973		20200512	14.0.409.0	
FireEye	✗	Trojan.GenericKD.41432973		20200508	32.31.0.0	
CAT-QuickHeal	✗	OLE.Encrypted.35277		20200512	14.00	
McAfee	✗	RDN/Generic.dx		20200512	6.0.6.653	



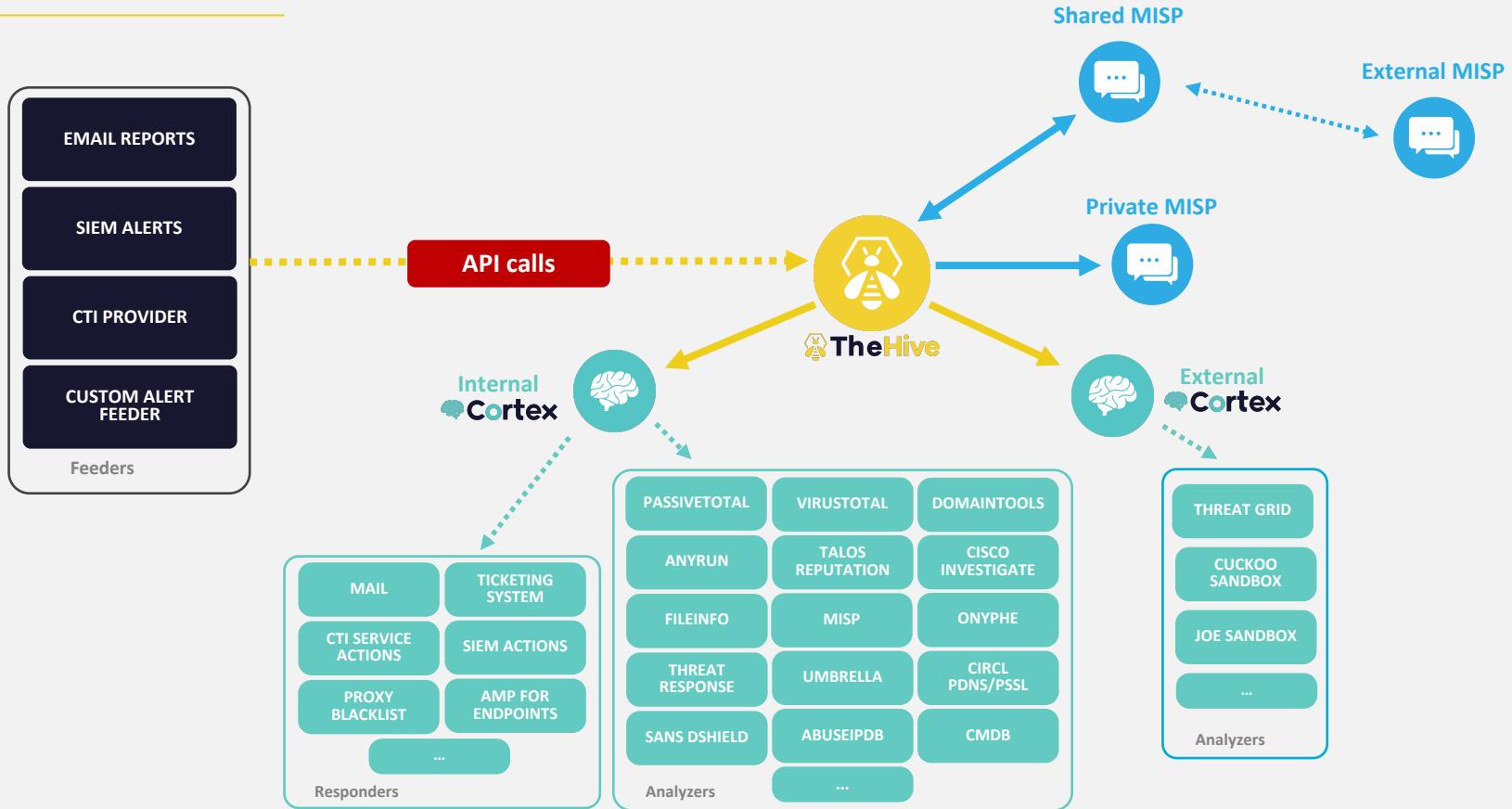
# Responders

---

- **Act on Alert, Case, Task, Log, Observable objects**
  - « Create a ticket in ticketing system »
  - « Add observable to Blacklist »
- **Input:** Data and metadata
- **Output 1:** action status Success or Failure
- **Output 2:** a set of **operations** to run in TheHive
  - « Add tags to Case/Observable »
  - « Add/Close a Task or a log »



# Typical Integration





## TheHive and SIEMs

# TheHive & SIEMs

---

64%

Of our users, integrate  
TheHive with a SIEM



# TheHive & Elastic Stack

---

- TheHive 3 and Cortex use Elasticsearch
- ELK is one of the most used SIEMs with TheHive
- Thanks to Elastalert and its “HIVE” connector

*“Easy & Flexible Alerting With Elasticsearch”*



- Integration can also be done through Watcher (x-Pack)
- And what about Elastic Security?



# TheHive & Elastic Stack

Definition   About   Schedule   **Actions**

## Actions

**Actions frequency**

On each rule execution

Select when automated actions should be performed if a rule evaluates as true.

**Actions**

>  SwiftCrypto Slack

>  SwiftCrypto JIRA

**Select an action type**

 Email    IBM Resilient    Jira    PagerDuty    ServiceNow    Slack    Webhook    TheHive

**One more possible solution ?**

 Cancel    Save changes

# TheHive & Elastic Stack

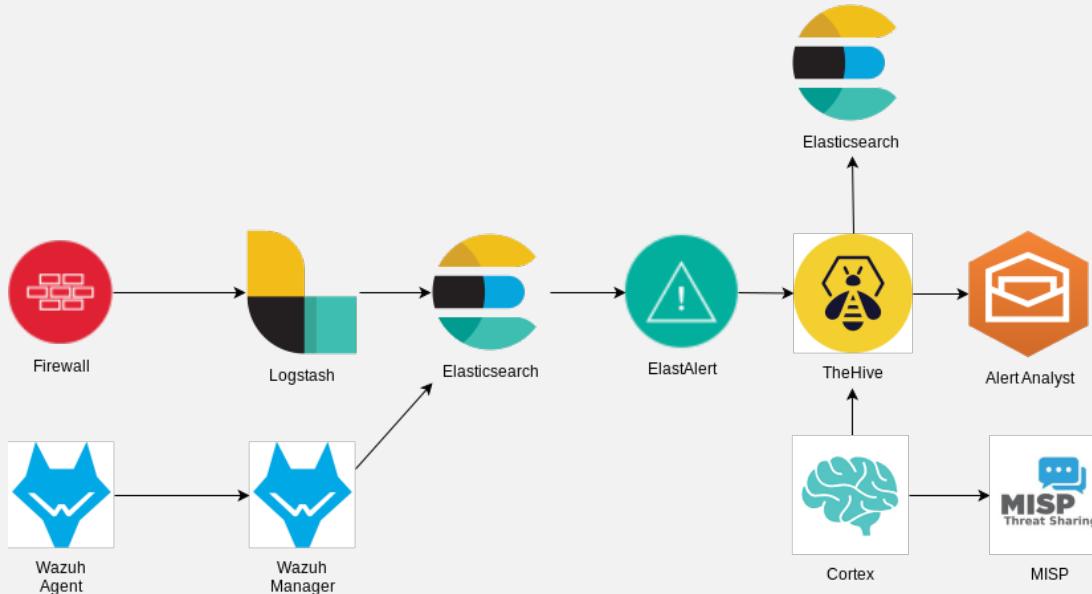
- Cortex has an ES analyzer, by Nick Prokop

Matches	
20 Hit(s)	
<a href="#">Copy query to clipboard</a>	
Kibana Dashboard:	2b644420-ec33-11ea-8850-65fd576fe3b8
10 User(s)	10 Device(s)
MNC	JIOWIN10.██████████
mth	MTH1WIN10.██████████
les	MNCWIN10.██████████
pja	KJAWIN10.██████████
paw	MGUWIN10.██████████

Timeline										
Time	User	Device	Parent → Process	Process Args	Dns Question Name	Dns Resolved IP	Source IP:Port	Destination IP:Port	Rule Category	Index
10/09/2020 05:52 AM	les	LESWIN10.██████████	chrome.exe → Ikke bekraeftet	670598.crdownload		192.168.1.100			Threat Detected	-amp-2020.10
10/09/2020 04:35 AM	pja	PJAWIN10.██████████	updater.exe → Viber.exe			192.168.8.103			Exploit Prevention	-amp-2020.10
10/08/2020 11:59 AM	emo	TLTWIN764.██████████	chrome.exe → f_0009ce			192.168.9.160			Threat Detected	-amp-2020.10
10/08/2020 08:23 AM	pep	PEPWIN10.██████████	explorer.exe → WinCDEmu-4.1.exe			192.168.23.143			Threat Detected	-amp-2020.10
10/06/2020 05:35 AM	paw	PAWWIN10.██████████	chrome.exe → f_0000a3			192.168.21.144			Threat Detected	-amp-2020.10
10/04/2020 02:48 PM	kja	KJAWIN10.██████████	explorer.exe → CanonFM.exe			192.168.1.58			Threat Detected	-amp-2020.10
10/04/2020 02:48 PM	kja	KJAWIN10.██████████	explorer.exe → CanonFM.exe			192.168.1.58			Threat Detected	-amp-2020.10
10/02/2020 10:58 AM	mth	MTH1WIN10.██████████	chrome.exe → f_00010f			192.168.56.1			Threat Detected	-amp-2020.10
10/02/2020 10:58 AM	mth	MTH1WIN10.██████████	chrome.exe → f_00010f			172.16.15.14			Threat Detected	-amp-2020.10
10/01/2020 07:32 PM	mgu	MGUWIN10.██████████	chrome.exe → f_004513			172.17.10.37			Threat Detected	-amp-2020.10
10/01/2020 07:32 PM	mgu	MGUWIN10.██████████	chrome.exe → f_004513			192.168.1.232			Threat Detected	-amp-2020.10
09/30/2020 10:57 AM	MNC	MNCWIN10.██████████	chrome.exe → libreoffice_0277735866.exe			172.17.10.72			Exploit Prevention	-amp-2020.09
09/30/2020 10:57 AM	MNC	MNCWIN10.██████████	chrome.exe → libreoffice_0277735866.exe			192.168.0.97			Exploit Prevention	-amp-2020.09

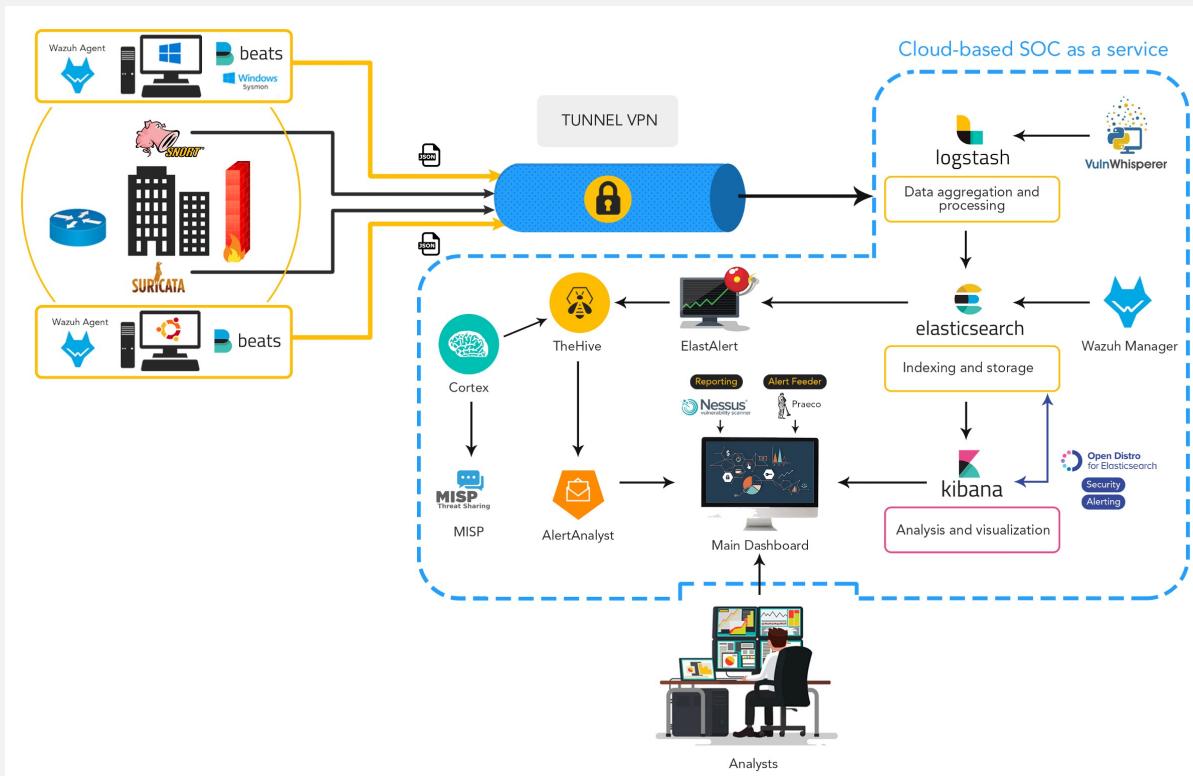


# TheHive & Elastic Stack - Examples



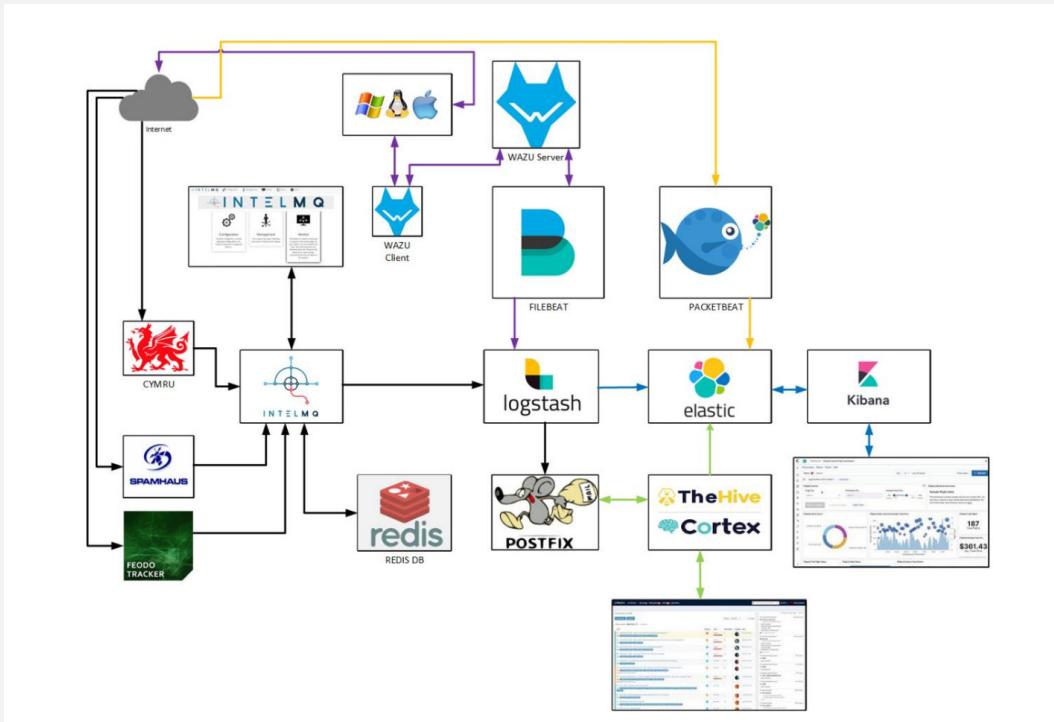
[Open Source SIRP with Elasticsearch and TheHive](#)

# TheHive & Elastic Stack - Examples



[Deploying of infrastructure and technologies for a SOC as a Service \(SOCaaS\)](#)

# TheHive & Elastic Stack - Examples



CSIRT TOOLS KIT

## TheHive & Elastic Stack – Blogs posts

---

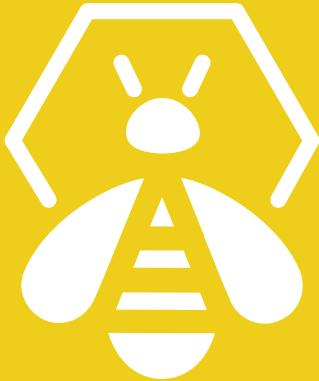
- Using Elasticsearch to Trigger Alerts in TheHive ([link](#))
- Deploying of infrastructure and technologies for a SOC as a Service ([link](#))
- Open Source SIRP with Elasticsearch and TheHive ([link](#))
- **SANS Webcast:** Hear me SOAR - Using Elastic, ElastAlert and TheHive in an effective purple team pipeline ([link](#))

## TheHive & Elastic Stack – Bundles

---

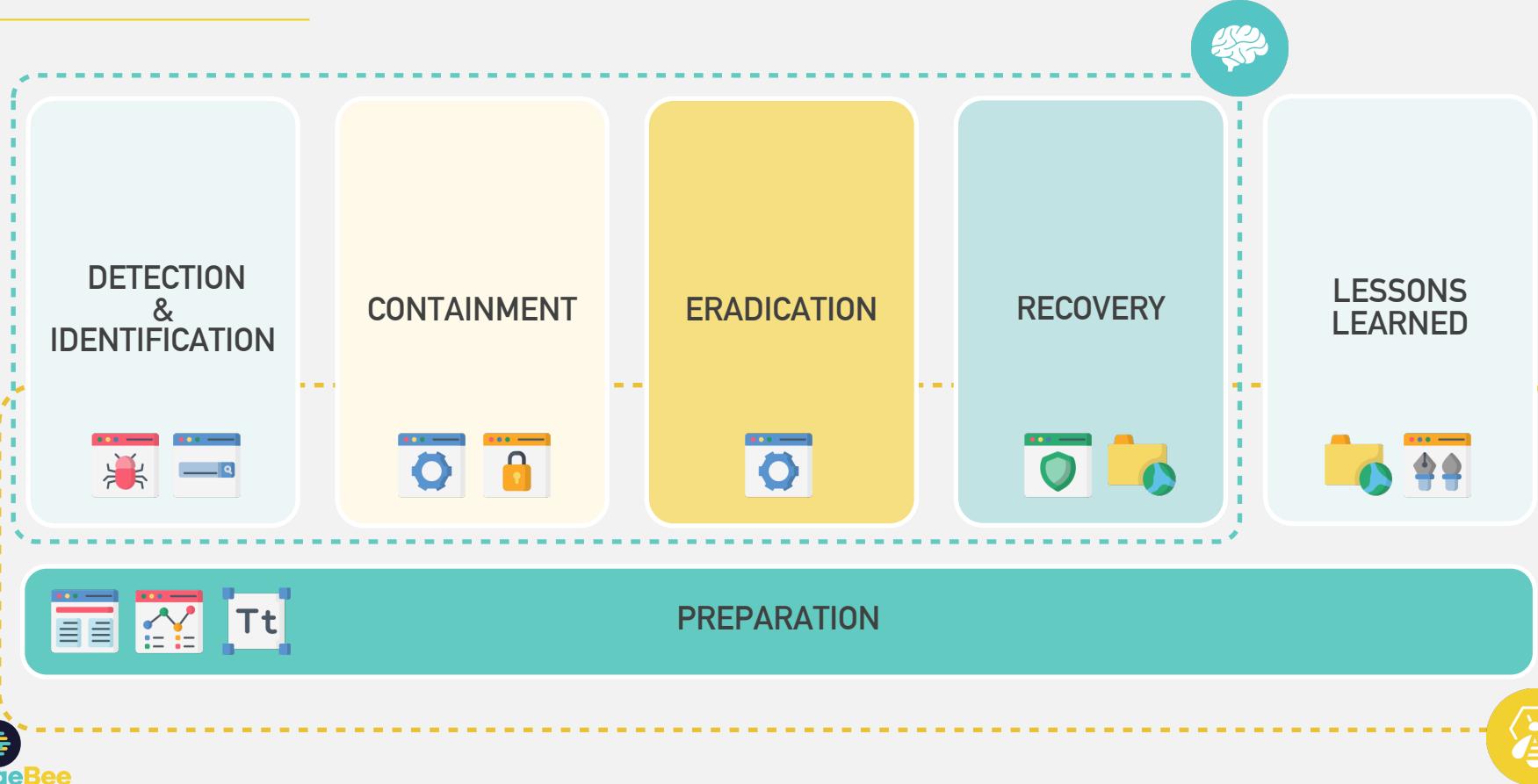
- Many projects include TheHive, Cortex and ELK as a bundled package:





# Incident Response using TheHive & Cortex

# Incident Response Process





## TheHive 4 features

# What's new with TheHive 4.0 ?

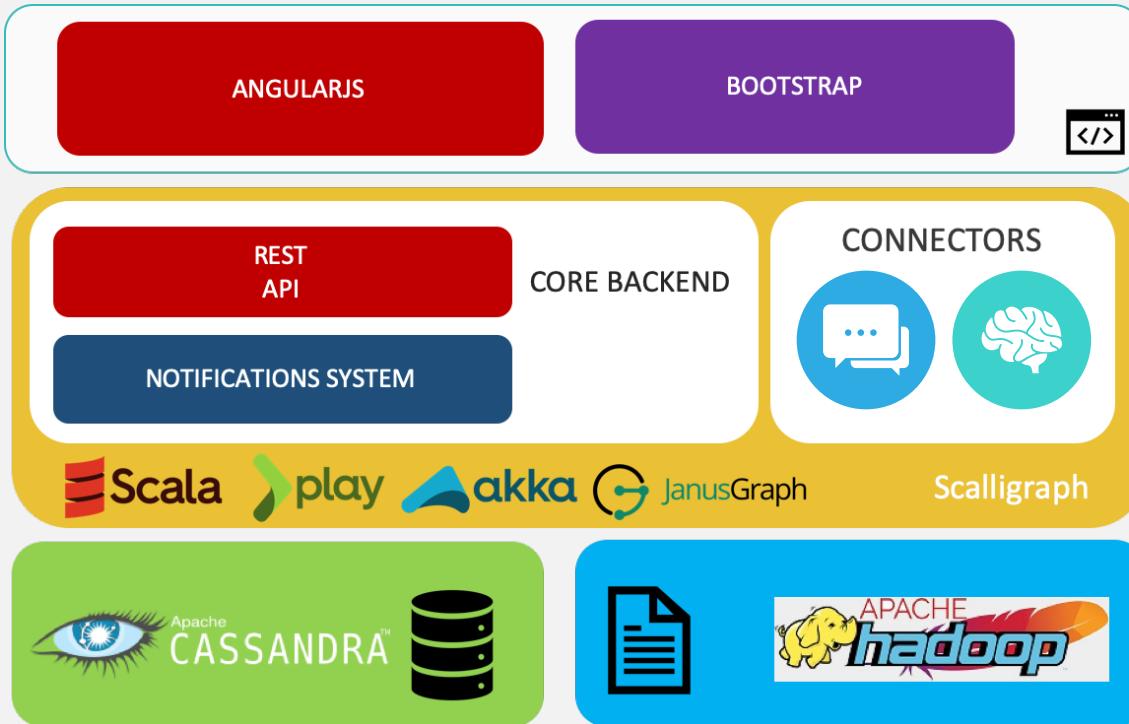
---

- Current version: TheHive 4.0.5 STABLE
- Complete rewrite of the backend
- Built with **multi-tenancy** support
- Custom roles and permissions, aka. **RBAC**
- Sharing and collaboration across organisations on cases and tasks
- UI improvements
- TheHive FS
- Two-Factor authentication
- Improved OAUTH2 support



# The Architecture

---



Front end

TheHive core application

Data



## A deep look into the new features

# Welcome to Organisations

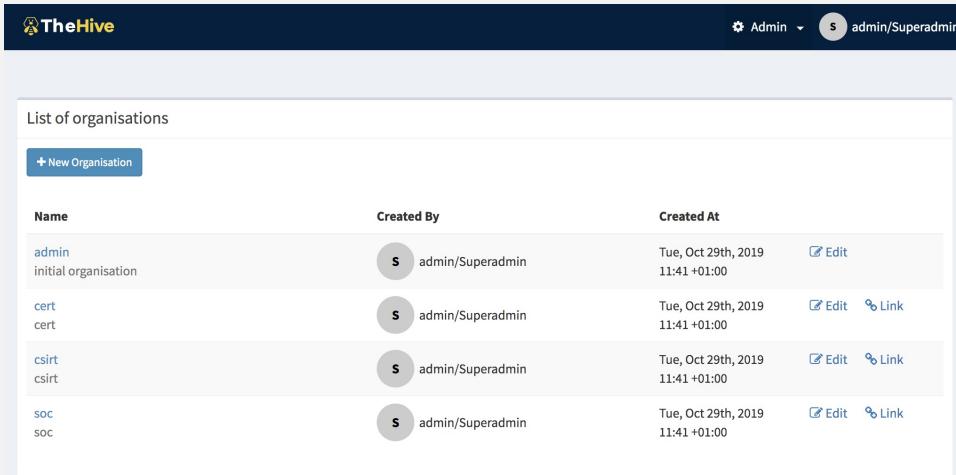
- An organisation

- Contains one or several users
- Defines what its users can do, can see (permissions)

- Organisation data is by default isolated

- Creates logic isolation of data
- An org can't access data that's not tied to it

- A user can belong to one or several organisations

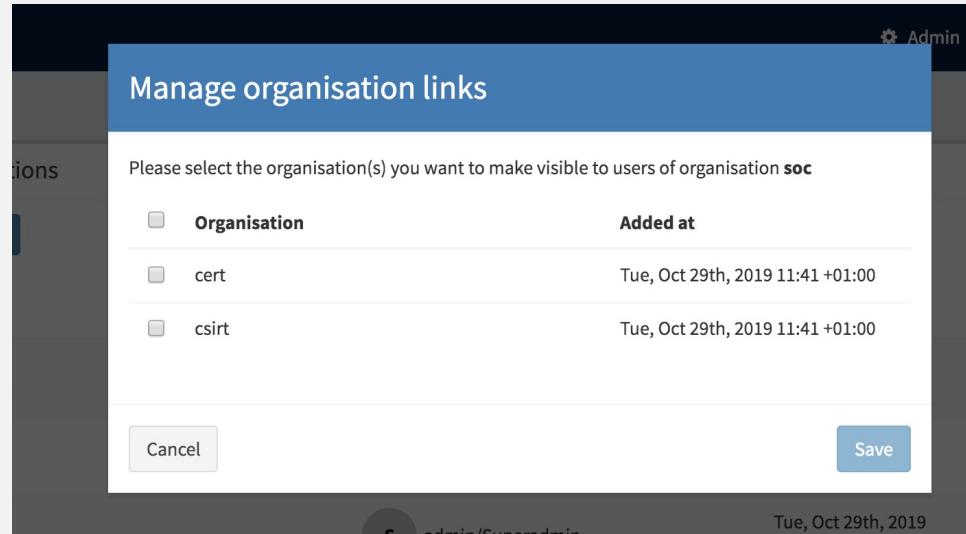


The screenshot shows the TheHive interface with a dark header bar. On the right side of the header, there is a user icon labeled "Admin" and "admin/Superadmin". The main content area has a light gray background and displays a table titled "List of organisations". The table includes a "New Organisation" button and columns for "Name", "Created By", and "Created At". The data in the table is as follows:

Name	Created By	Created At	Actions
admin initial organisation	 admin/Superadmin	Tue, Oct 29th, 2019 11:41 +01:00	 
cert cert	 admin/Superadmin	Tue, Oct 29th, 2019 11:41 +01:00	 
csirt csirt	 admin/Superadmin	Tue, Oct 29th, 2019 11:41 +01:00	 
soc soc	 admin/Superadmin	Tue, Oct 29th, 2019 11:41 +01:00	 

# Organisation Visibility

- Super administrators can define which organisation can collaborate with which one
- An organisation must be ‘linked’ to other organisations to be able to share data (cases/tasks) with them
- ‘linking’ is a temporary term



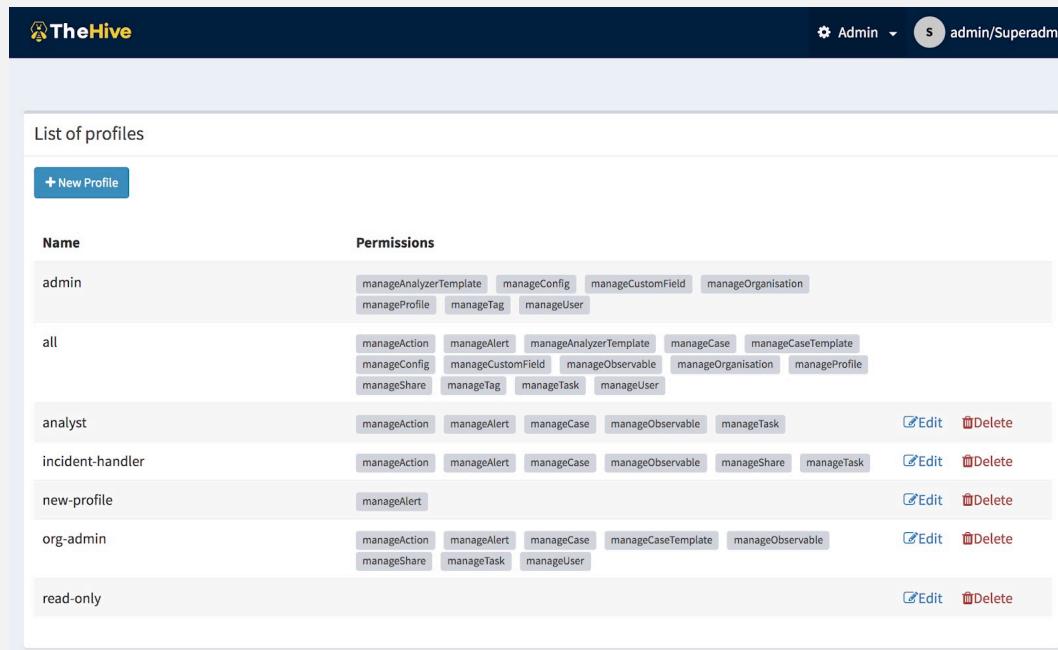
The screenshot shows a modal window titled "Manage organisation links". The header includes a gear icon, "Admin", and a close button. The main content area has a blue header bar with the title. Below it, a message says "Please select the organisation(s) you want to make visible to users of organisation **soc**". A table lists three organisations with checkboxes:

Organisation	Added at
cert	Tue, Oct 29th, 2019 11:41 +01:00
csirt	Tue, Oct 29th, 2019 11:41 +01:00

At the bottom are "Cancel" and "Save" buttons.

# Profiles and Permissions

- **TheHive** comes with a set of predefined permissions
- A **Profile** is a set of **Permissions**
- A user has a **Profile** on an Organisation (can be different from ORG1 to ORG2)
- Profiles are used to define the sharing boundaries. Example: share a case as *Read-Only*



Name	Permissions	Edit	Delete
admin	manageAnalyzerTemplate manageConfig manageCustomField manageOrganisation manageProfile manageTag manageUser	<input type="checkbox"/>	<input type="checkbox"/>
all	manageAction manageAlert manageAnalyzerTemplate manageCase manageCaseTemplate manageConfig manageCustomField manageObservable manageOrganisation manageProfile manageShare manageTag manageTask manageUser	<input type="checkbox"/>	<input type="checkbox"/>
analyst	manageAction manageAlert manageCase manageObservable manageTask	<input type="checkbox"/>	<input type="checkbox"/>
incident-handler	manageAction manageAlert manageCase manageObservable manageShare manageTask	<input type="checkbox"/>	<input type="checkbox"/>
new-profile	manageAlert	<input type="checkbox"/>	<input type="checkbox"/>
org-admin	manageAction manageAlert manageCase manageCaseTemplate manageObservable manageShare manageTask manageUser	<input type="checkbox"/>	<input type="checkbox"/>
read-only		<input type="checkbox"/>	<input type="checkbox"/>

## Collaboration and Sharing

---

- Sharing = “Make an object **I own, visible** by an Organisation **I trust.**”
- Mechanism that allows two or more organisations to collaborate
- Sharing is possible for Cases, Tasks and Observables
- Requires *manageShare* permission
- For Cases, there is a dedicated tab in case details page
- For Tasks/Observables , there is a dedicated section within the Task/Observable details page

# Collaboration and Sharing - Cases

The screenshot shows the TheHive interface for managing cases. At the top, there is a navigation bar with links for 'New Case', 'My tasks (1)', 'Waiting tasks (1)', 'Alerts (3)', 'Dashboards', 'Search', 'Organisation', and a user profile for 'cert/Nabil Adouani'. Below the navigation bar, a specific case is displayed: 'Case # 33 - New Alert' was created by Nabil Adouani on Tuesday, Oct 29th, 2019 at 14:32 +01:00, with 1 alert. The case has five observables. A red box highlights the 'Sharing' button in the top right corner of the case details panel. Below the sharing button are standard case actions like 'Close', 'Flag', 'Merge', 'Remove', and 'Responders'. At the bottom of the panel, there are buttons for 'Action', 'Add observable(s)', 'Export', 'Stats', 'Filters', and a 'per page' dropdown set to 15.

# Collaboration and Sharing - Cases

The screenshot shows the TheHive interface with a 'Share case' dialog box overlaid. The dialog box is titled 'Share case' and contains instructions: 'Select the organisations you would like to share the case with.' It has sections for 'Organisation\*', 'Profile\*', 'Tasks\*', and 'Observables\*'. The 'Organisation\*' section has a dropdown menu with 'soc' selected. The 'Profile\*' section has a dropdown menu with 'incident-handler' selected. The 'Tasks\*' section has a dropdown menu with 'all' selected. The 'Observables\*' section has a dropdown menu with 'none' selected. At the bottom are 'Cancel' and 'Save' buttons.

TheHive

+ New Case My tasks 1 Waiting tasks 1 Alerts 3 Dashboards Search

Caselid Organisation cert/Nabil Adouani

Case # 32 - [MISP]Sample 2

Created by Nabil Adouani Tue, Oct 29th, 2019 12:00:00

Details Tasks 2 Observables

+ Add share

The current case is shared with the following organisation:

Organisation

csirt

Share case

Select the organisations you would like to share the case with.

Organisation \*

soc

Profile \*

incident-handler

Tasks \*

all

Observables \*

none

Shared At Actions

11/04/19 17:11 Delete

Cancel Save

# UI Improvements

- RBAC adaptative UI: menus and actions rely on user permissions

As an organisation administrator



As a read-only user



# Enhanced Alert Triage

- Reviewed Alert observables section: pagination + filters + performance
- Support for *ignoreSimilarity* flag observables

Alert Preview New

**M** create\_alert\_observable  
ID: ~41074688 Date: Wed, Feb 3rd, 2021 15:26 +01:00 Type: external Reference: d88544 Source: development  
ais-marking:TLPMarking="GREEN" thehive4py debug

Description

New Description

Additional fields Layout

No additional information have been specified

Observables 2 Similar cases 1

Filters 15 per page

**Filters**

dataType any of file Enter a dataType

+ Add a filter Clear

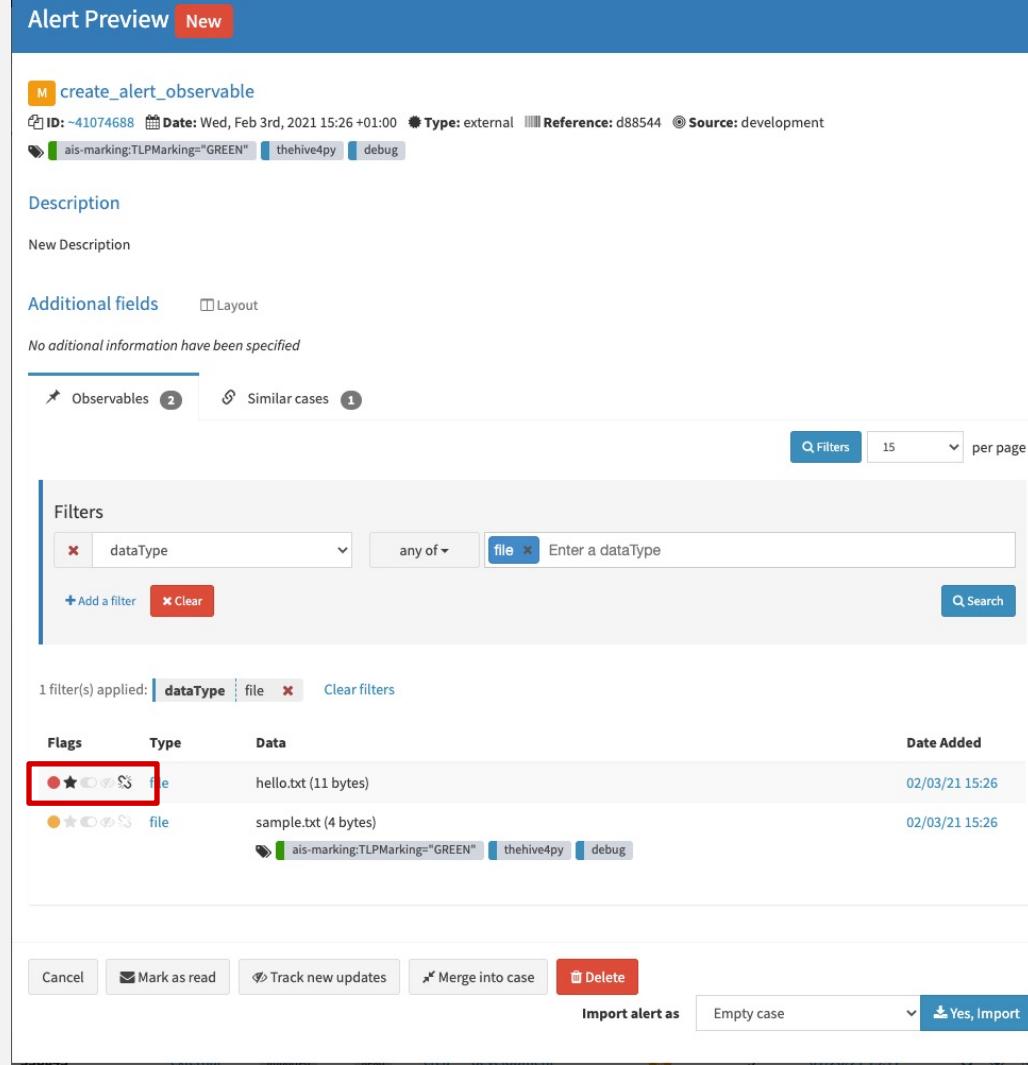
Search

1 filter(s) applied: dataType file Clear filters

Flags	Type	Data	Date Added
<span style="color: red;">●</span> <span style="color: orange;">★</span> <span style="color: green;">○</span> <span style="color: blue;">○</span> <span style="color: purple;">○</span> <span style="color: yellow;">○</span> <span style="color: cyan;">○</span> <span style="color: magenta;">○</span>	file	hello.txt (11 bytes)	02/03/21 15:26
<span style="color: orange;">●</span> <span style="color: green;">★</span> <span style="color: green;">○</span> <span style="color: blue;">○</span> <span style="color: purple;">○</span> <span style="color: yellow;">○</span> <span style="color: cyan;">○</span> <span style="color: magenta;">○</span>	file	sample.txt (4 bytes)	02/03/21 15:26

Cancel Mark as read Track new updates Merge into case Delete

Import alert as Empty case Yes, Import



# Enhanced Alert Triage

- Reviewed Alert similar cases section:

- Pagination
- Filters
- Matched observable types

- Support for *ignoreSimilarity* flag observables

Alert Preview New

M create\_alert\_observable  
ID: ~41074688 Date: Wed, Feb 3rd, 2021 15:26 +01:00 Type: external Reference: d88544 Source: development  
ais-marking:TLPMarking="GREEN" thehive4py debug

Description  
New Description

Additional fields Layout  
No additional information have been specified

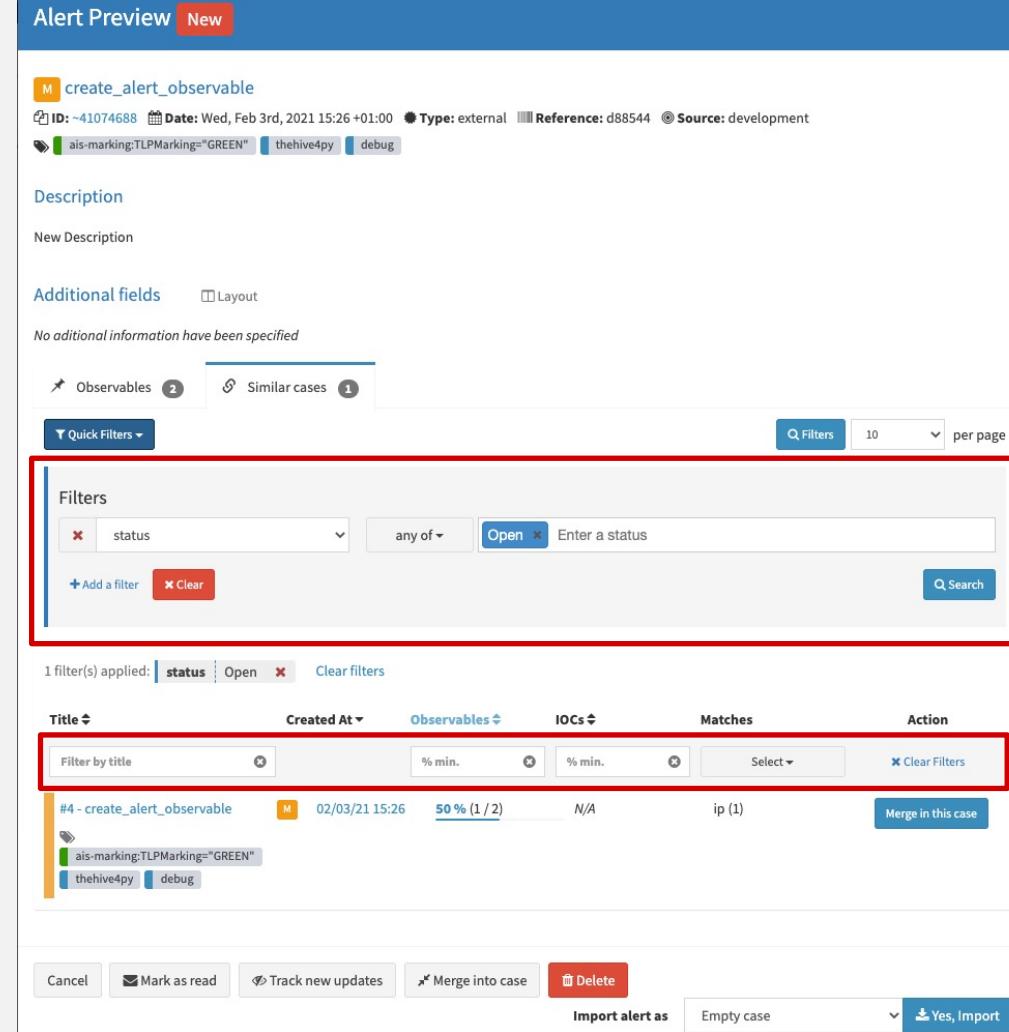
Observables 2 Similar cases 1 Quick Filters Q Filters 10 per page

**Filters**  
status any of Open Enter a status Add a filter Clear Search

1 filter(s) applied: status Open Clear filters

Title	Created At	Observables	IOCs	Matches	Action
#4 - create_alert_observable	02/03/21 15:26	% min. % min. Select	N/A	ip (1)	Merge in this case
ais-marking:TLPMarking="GREEN"	thehive4py debug				

Cancel Mark as read Track new updates Merge into case Delete Import alert as Empty case Yes, Import



# UI Improvements

- Using API v1
- Better search forms
- Allow filtering by custom fields and all possible attributes
- Same as *Search* sections

The screenshot shows the TheHive platform's search interface. At the top, there is a navigation bar with links for 'New Case', 'My tasks (1)', 'Waiting tasks (1)', 'Alerts (3)', 'Dashboards', 'Search', 'CaseId', 'Organisation', and a user profile for 'cert/Nabil Adouani'. Below the navigation bar, the main area displays a list of alerts with the heading 'List of alerts (3 of 4)'. There are three alert cards shown, each with a title and a snippet of information. Above the alert cards, there are several filter options: 'status' (set to 'any of' with 'New' and 'Updated' selected), 'tlp' (set to 'any of' with 'red' and 'amber' selected), 'severity' (set to 'any of' with 'high' selected), 'title' (set to 'any of' with 'Alert\*' selected), and 'date' (set to 'any of' with a range from '01-11-2019' to '12-11-2019'). At the bottom of the filter section, there are buttons for '+ Add a filter' and 'Clear'. Below the filters, a summary of applied filters is shown: 'status: New, Updated', 'tlp: red, amber', 'severity: high', 'title: Alert\*', and 'date: From: 11/01/19 00:00, To: 11/12/19 23:59'. A 'Clear filters' button is also present.

# UI Improvements

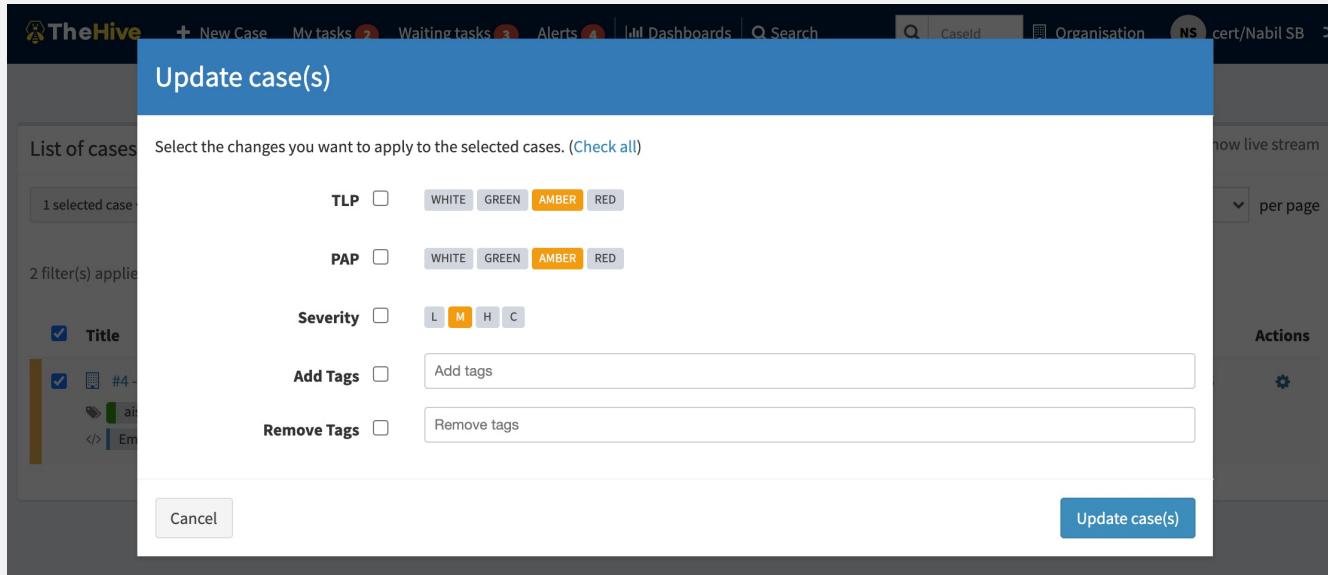
- Display custom fields in case and alert list + quick filtering by custom fields

The screenshot shows the TheHive interface. At the top, there's a navigation bar with links for 'New Case', 'My tasks (2)', 'Waiting tasks (3)', 'Alerts (4)', 'Dashboards', 'Search', 'CaseId', 'Organisation', and a user profile 'cert/Nabil SB'. Below the navigation is a search bar and a 'Custom Fields' button, which is highlighted with a red box. Further down, there's a 'List of cases (1 of 5)' section with filters for 'tags' and 'customFields.email-from'. Another red box highlights the 'Email From' filter. The main area displays a table of cases with columns for 'Severity', 'Tasks', 'Observables', 'Assignee', 'Date', and 'Actions'. One specific case is highlighted with a red box, showing its details: severity 'M', 3 tasks, 5 observables, assigned to 'NS', created on '02/03/21 15:26', and a status of 'a day'. The case title is '#4\_create\_alert\_observable'.

Severity	Tasks	Observables	Assignee	Date	Actions
M	3 Tasks	5	NS	02/03/21 15:26	
<p>#4_create_alert_observable</p> <p>ais-marking:TLPMarking="GREEN" thehive4py debug</p> <p>Email From: nabil@strangebee.com Ticket Status: Open</p>					

# UI Improvements

- Bulk operations in case and observable lists



# UI Improvements

- Visual statistics in case, alert, observable lists

TheHive UI screenshot showing visual statistics and case lists.

Header:

- New Case
- My tasks (2)
- Waiting tasks (3)
- Alerts (4)
- Dashboards
- Search
- Caselid
- Organisation
- cert/Nabil SB

Top navigation bar:

- Quick Filters
- Sort by
- Custom Fields
- Stats
- Filters
- 15 per page

Section: List of cases (1 of 5)

Statistics:

- Case by Status: Open (blue), Resolved (orange)
- Case by Resolution: Indeterminate (blue)
- Top 5 tags: debug (blue), thehive4py (red), ais-marking:TLPMarking="GREEN" (yellow), PAP="GREEN" (teal), europol-event="file-inclusion-attempt" (dark blue)

Filter applied: tags the\* customFields.email-from nabil@strangebee.com

Table: Case list

Title	Severity	Tasks	Observables	Assignee	Date	Actions
#4 - create_alert_observable ais-marking:TLPMarking="GREEN" thehive4py debug Email From: nabil@strangebee.com Ticket Status: Open	Info	3 Tasks	5	NS	02/03/21 15:26 a day	

# TheHive FS

- Get quick access to files stored in TheHive directly from your investigation machine
- Connect remote webdav FS of TheHive  
`dav(s)://thehive:9001/fs`
- Use credentials of TheHive user
- Speed up investigation & analysis (but try not to step on a landmine)

The screenshot shows the TheHive FS interface. At the top, there's a header for "Case # 40 - Malware detected by AV in a desktop" created by "certuser" on "Fri, Oct 25th, 2019 15:36 +02:00". Below the header are tabs for "Details", "Tasks" (with 1 item), "Observables" (with 2 items), and "Forensics" (with 3 items). A toolbar below the tabs includes "Action", "+ Add observable(s)", and "Export".  
  
The main area is titled "Observable List (2 of 2)" and contains two entries:

Type	Value/Filename
file	Carbone4[.]jar None No reports available
ip	195[.]195[.]2[.]13 None No reports available

  
On the right, there's a file browser window titled "cases 40 observables". It shows a list of files and folders:

Name	Size	Modified
37	—	22 oct. 2019
38	—	23 oct. 2019
39	—	28 oct. 2019
40	—	28 oct. 2019
observables	—	02:53
Carbone4.jar	55,2 kB	02:51
tasks	—	02:53
Desktop_screenshot1.png	6,6	"40" selected

The folder "40" is currently selected.

# 2FA Authentication

- Users can enable 2FA authentication
- Compatible with authenticator apps
- Administrators can see who has enabled the 2FA authentication

Enable Multi-Factor Authentication

Your are going to enable Multi-Factor Authentication. Use the QRCode or the Secret to generate a MFA code and submit it.

Need a two-step authenticator app? Download one of the following  
iOS devices: [Authy](#)  
Android devices: [Authy](#)  
Windows devices: [Microsoft Authenticator](#)



TCIH7ZNLKFUJYTNXU26KYDC

[!\[\]\(1895fb545c2067159fac3474302cf280\_img.jpg\) Copy secret](#)

**Code \***

[Cancel](#) \* Required field

TheHive

Sign in to start your session

nabil@strangebee.com

•••••

Please provide MFA code

Code

Sign In

OR

Sign In with SSO

# Single Sign On

- TheHive administrator can enable SSO via an OAuth2 configuration
- Compatible with many providers and services: Okta, MS365, Keycloak, FusionAuth, Google OpenID...



Sign in to start your session

👤

🔒

Sign In

---

OR

Sign In with SSO

# StrangeBee

Need Help?



# Thank You, any questions?

## Community



<https://blog.thehive-project.org>



<https://chat.thehive-project.org>



[https://twitter.com/TheHive\\_Project](https://twitter.com/TheHive_Project)



[users@thehive-project.org](mailto:users@thehive-project.org)



<https://www.strangebee.com>



[contact@strangebee.com](mailto:contact@strangebee.com)