TLP:WHITE

RandoriSec & Friends 2020

TheHive 4

New features & Roadmap

Nabil Adouani

Co-founder of **TheHive** Project
@nadouani
@TheHive_Project

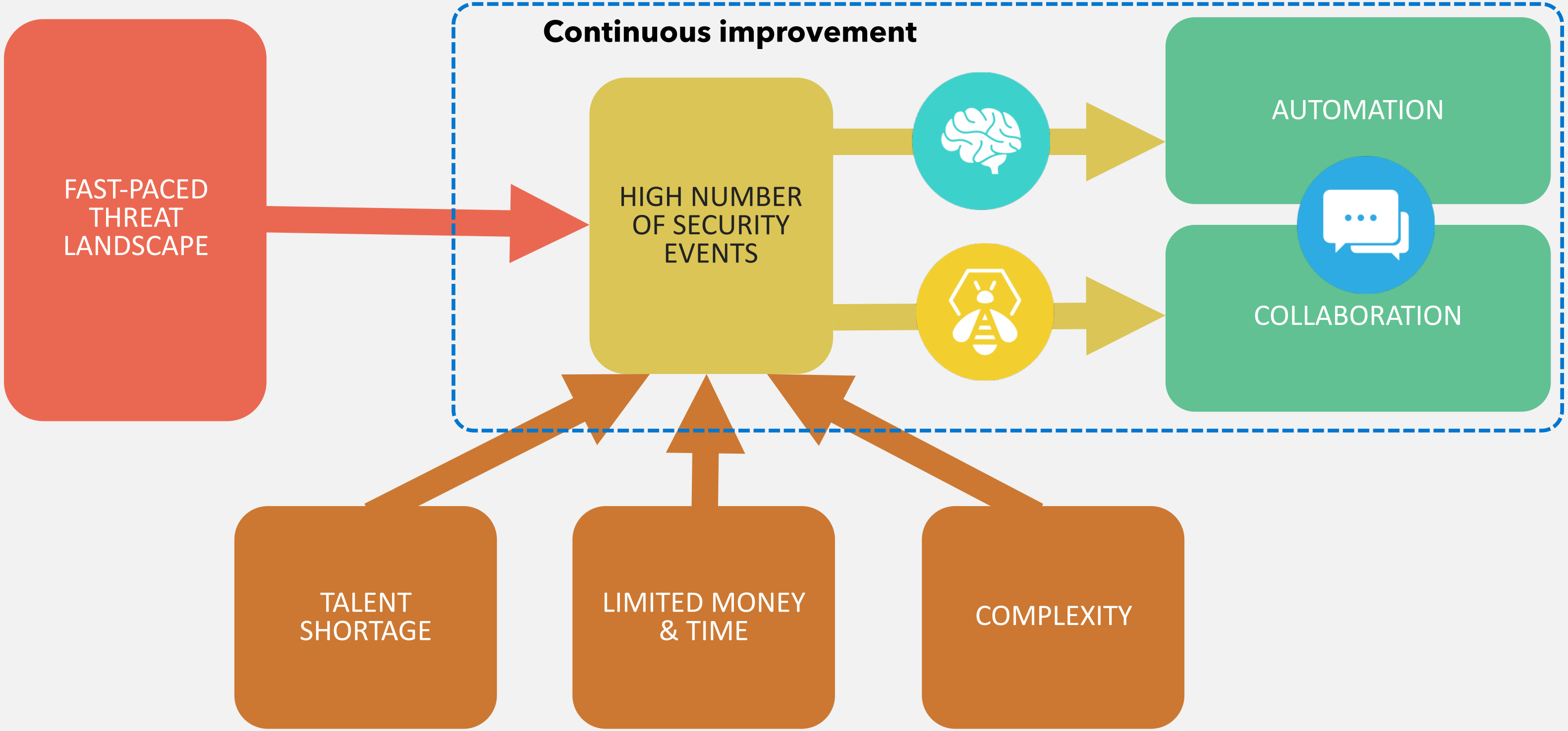
StrangeBee

The Agenda

- Story and timeline
- A wink to **MISP** Project
- **TheHive** from 3 to 4
- A deeper look into the new features
- Roadmap and future features
- Need help?

TheHive Project: Story and Timeline

Drive Down The Time to React



Continuous improvement

FAST-PACED THREAT LANDSCAPE

HIGH NUMBER OF SECURITY EVENTS

AUTOMATION

COLLABORATION

TALENT SHORTAGE

LIMITED MONEY & TIME

COMPLEXITY

The Timeline

- **February 2014**: First TheHive specifications
- **October 2014**: First private version
- **November 2016**: TheHive Project made public
- **February 2017**: Cortex v1 made standalone
- **March 2018**: Cortex v2 unveiled
- **October 2018**: 100+ Cortex Analyzers
- **Mars 2019**: TheHive **4** RC1 **Beta**
- **Mai 2019**: TheHive **4**, first release **Stable**

StrangeBee

What’s TheHive ?

TheHive is a **scalable**, **open source** and **free** Security Incident Response Platform

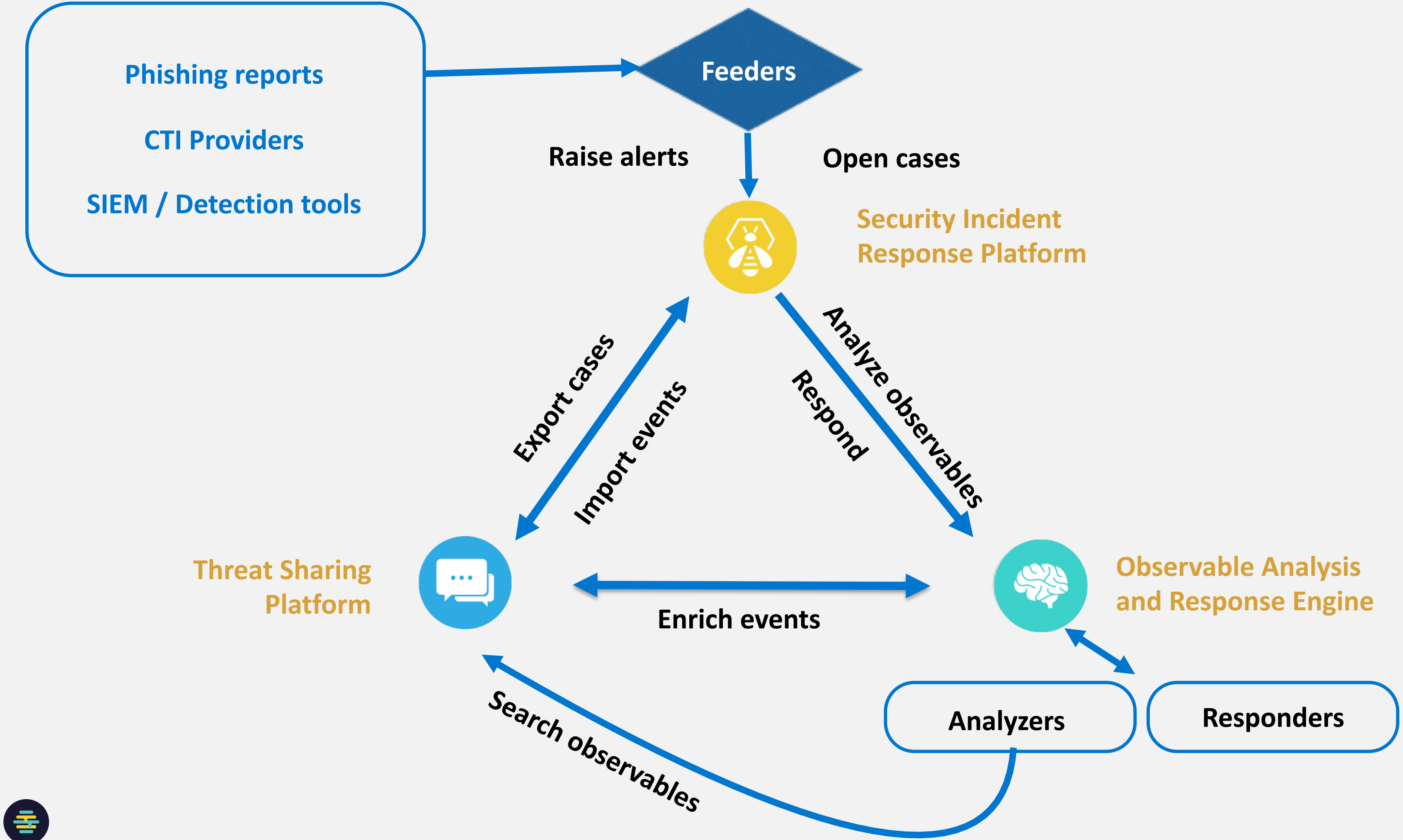
What’s Cortex ?

Cortex is a **scalable, open source** and **free** Observable Analysis and Active Response Platform

What’s MISP ?

MISP is an **open source** and **free** Threat Intelligence Platform

How do they work together?



Phishing reports

CTI Providers

SIEM / Detection tools

Feeders

Raise alerts

Open cases

Security Incident Response Platform

Export cases

Import events

Respond

Analyze observables

Threat Sharing Platform

Enrich events

Observable Analysis and Response Engine

Analyzers

Responders

Search observables

StrangeBee

TheHive, from 3 to 4

StrangeBee

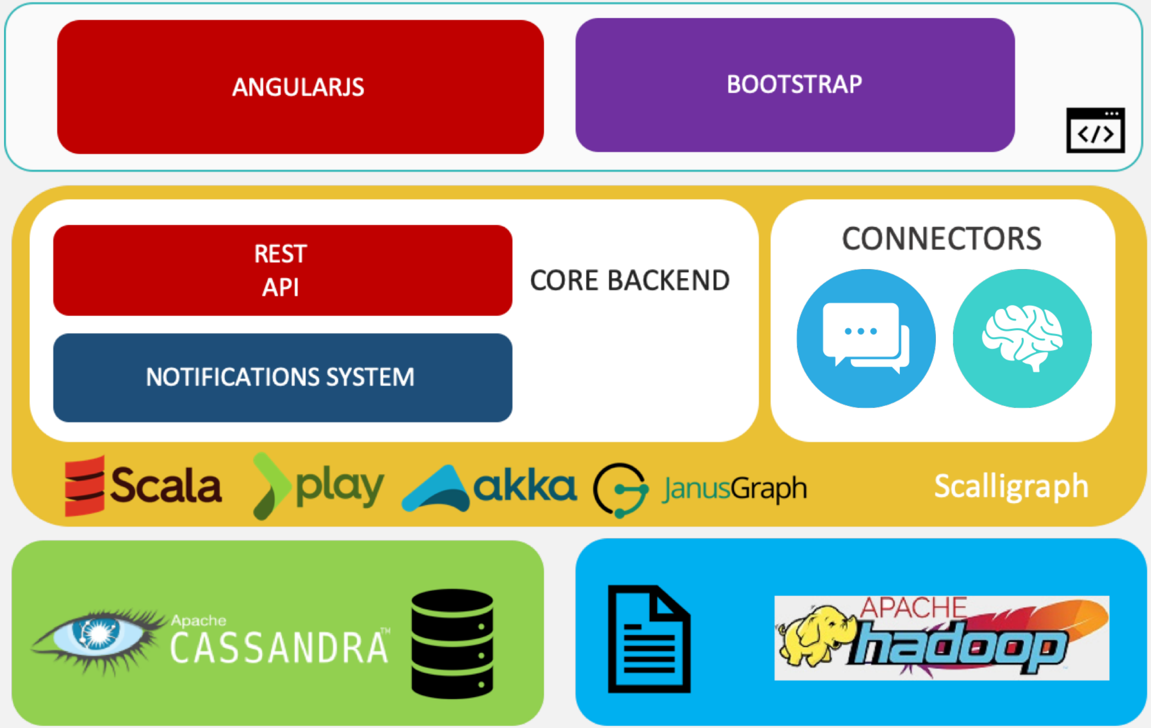
The Current Status

- Latest version: **TheHive** 3.4.x
- Suitable for flat teams
- Basic permissions (read, write, admin)
- Mono-Tenant
- Use Elasticsearch as database

The Promise of TheHive 4.0

- Current version: TheHive RC1
- Complete rewrite of the backend, still using Scala ❤
- Built to be used by multiple organisations, aka. **multi-tenancy**
- Custom roles and permissions, aka. **RBAC**
- Sharing and collaboration across organisations on cases and tasks
- UI improvements
- TheHive FS
- Two-Factor authentication (Work In Progress for 4.0 stable release)

The Architecture



Front end

TheHive core application

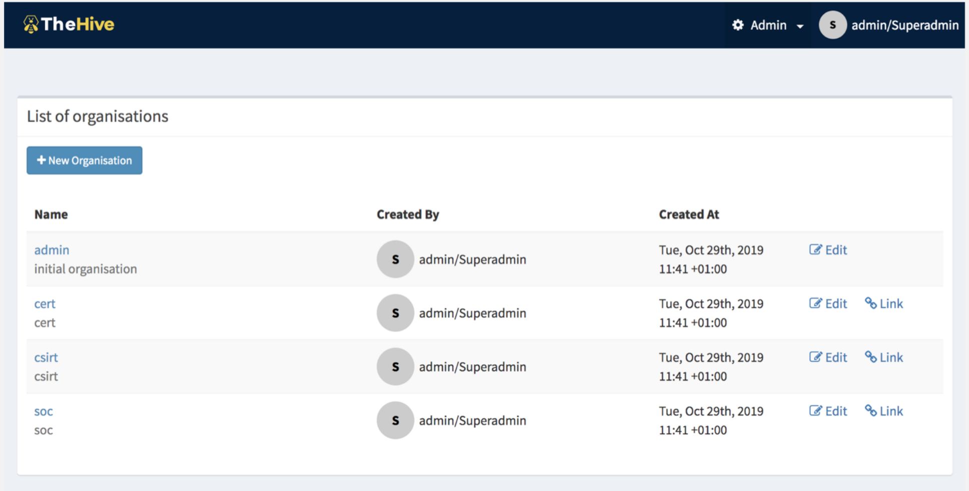
Data

StrangeBee

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



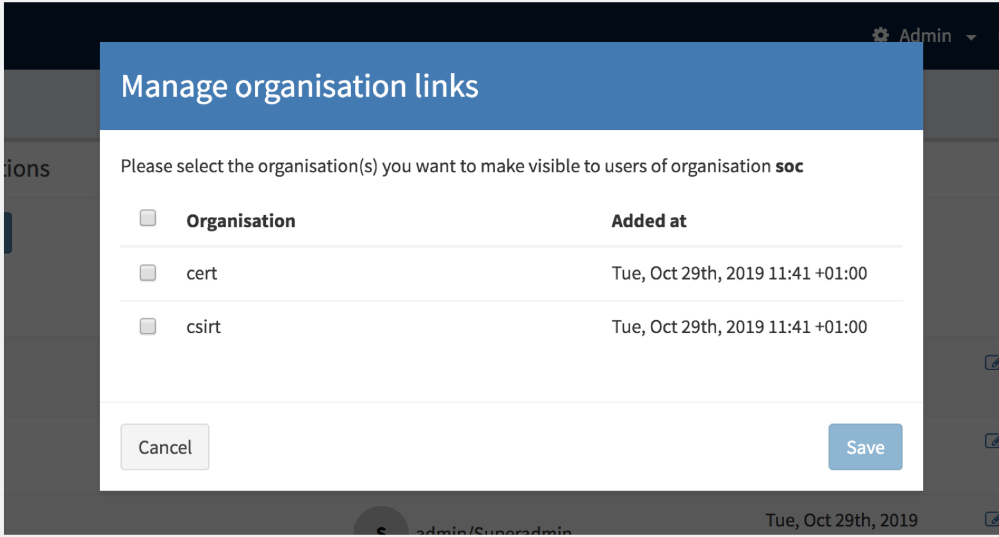
List of organisations

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

StrangeBee

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



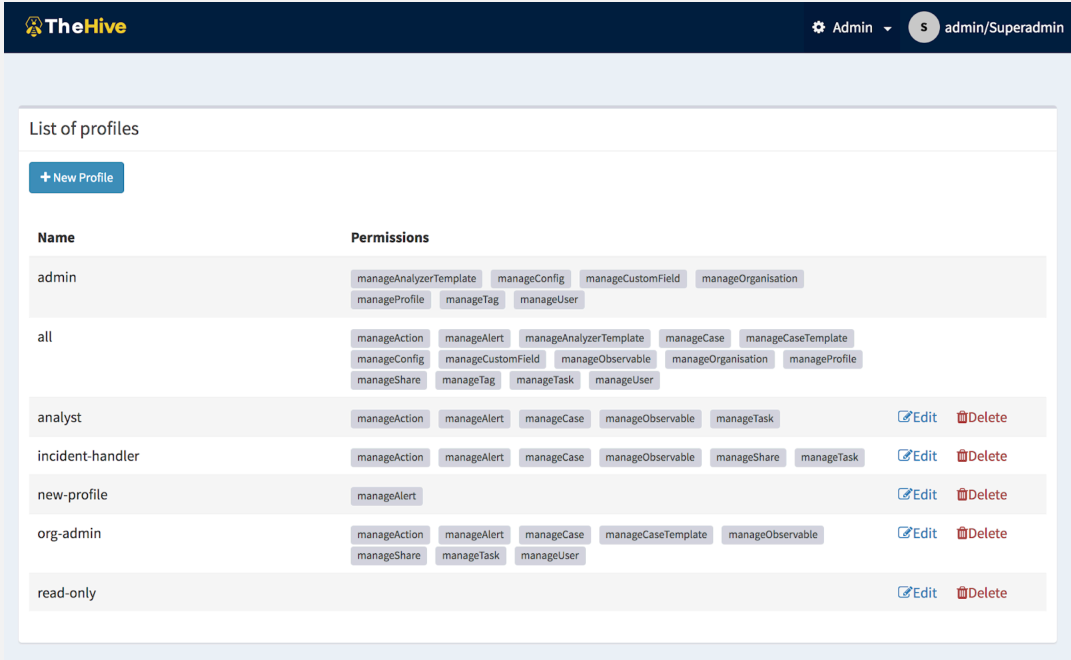
Manage organisation links

Please select the organisation(s) you want to make visible to users of organisation **soc**

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

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*



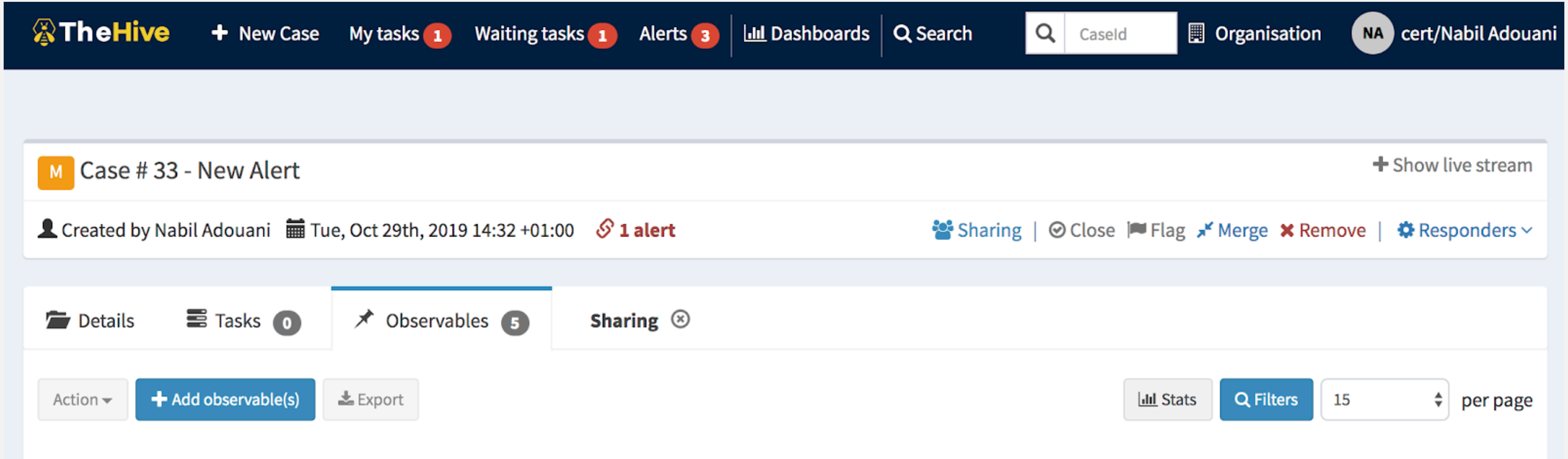
List of profiles

Name	Permissions		
admin	manageAnalyzerTemplate manageConfig manageCustomField manageOrganisation manageProfile manageTag manageUser		
all	manageAction manageAlert manageAnalyzerTemplate manageCase manageCaseTemplate manageConfig manageCustomField manageObservable manageOrganisation manageProfile manageShare manageTag manageTask manageUser		
analyst	manageAction manageAlert manageCase manageObservable manageTask	Edit	Delete
incident-handler	manageAction manageAlert manageCase manageObservable manageShare manageTask	Edit	Delete
new-profile	manageAlert	Edit	Delete
org-admin	manageAction manageAlert manageCase manageCaseTemplate manageObservable manageShare manageTask manageUser	Edit	Delete
read-only		Edit	Delete

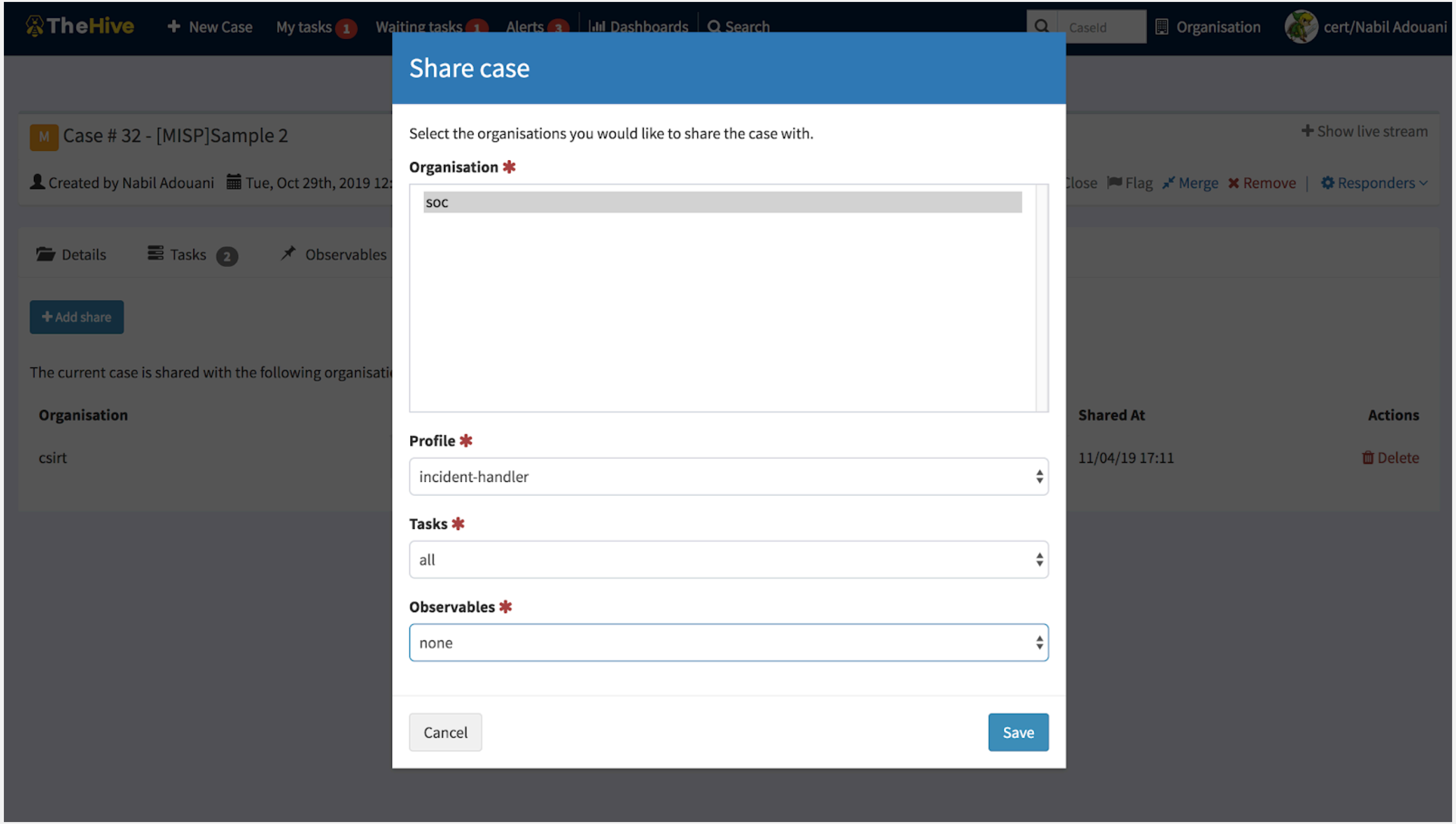
Collaboration and Sharing

- Sharing = “Make an object **I own**, **visible** by an Organisation **I trust**.”
- Mecanism that allow 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



Collaboration and Sharing - Cases



M Case # 32 - [MISP]Sample 2

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

The current case is shared with the following organisati

Organisation	Shared At	Actions
csirt	11/04/19 17:11	Delete

Share case

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

Organisation *

soc

Profile *

incident-handler

Tasks *

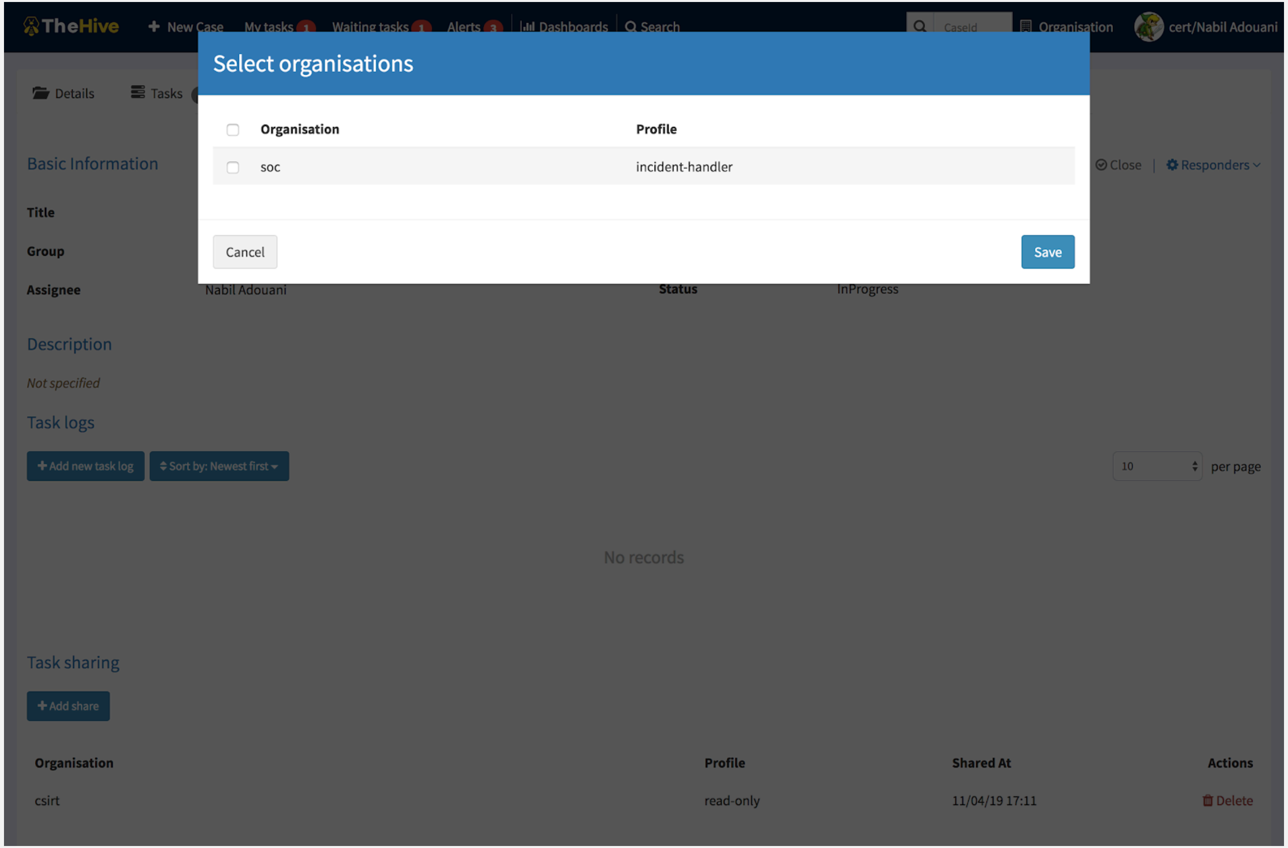
all

Observables *

none

Cancel | Save

Collaboration and Sharing - Tasks



Select organisations

□	Organisation	Profile
□	soc	incident-handler

Basic Information

Title

Group

Assignee: Nabil Adouani

Status: InProgress

Description

Not specified

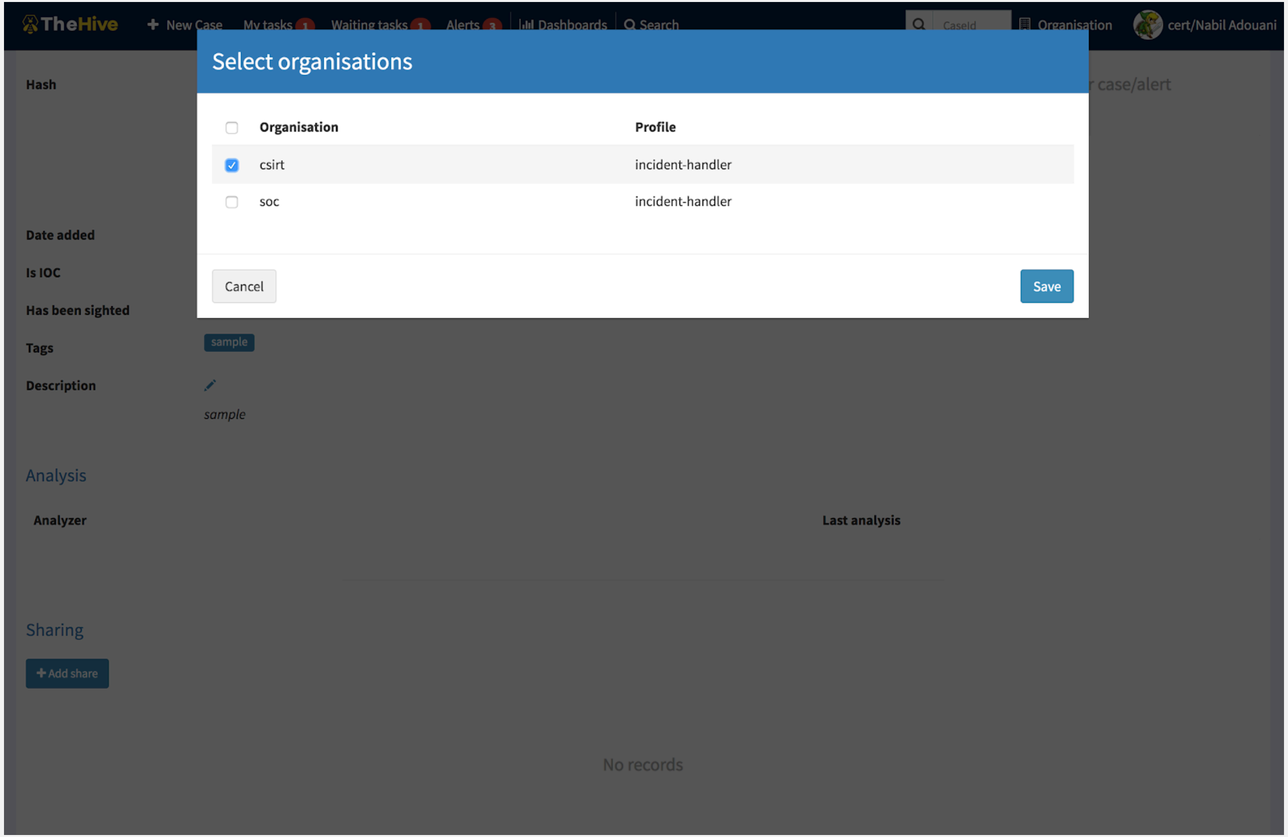
Task logs

No records

Task sharing

Organisation	Profile	Shared At	Actions
csirt	read-only	11/04/19 17:11	Delete

Collaboration and Sharing - Observables



Select organisations

☐	Organisation	Profile
☑	csirt	incident-handler
☐	soc	incident-handler

Hash

Date added

Is IOC

Has been sighted

Tags: sample

Description

sample

Analysis

Analyzer	Last analysis

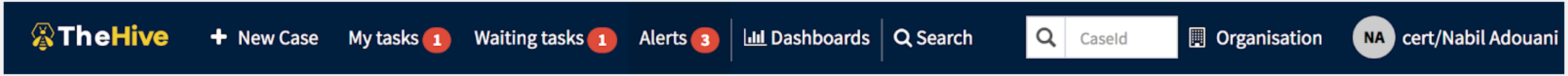
Sharing

No records

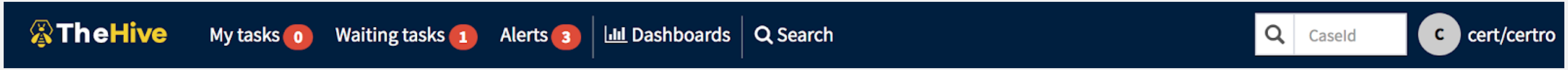
UI Improvements

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

As an organisation administrator

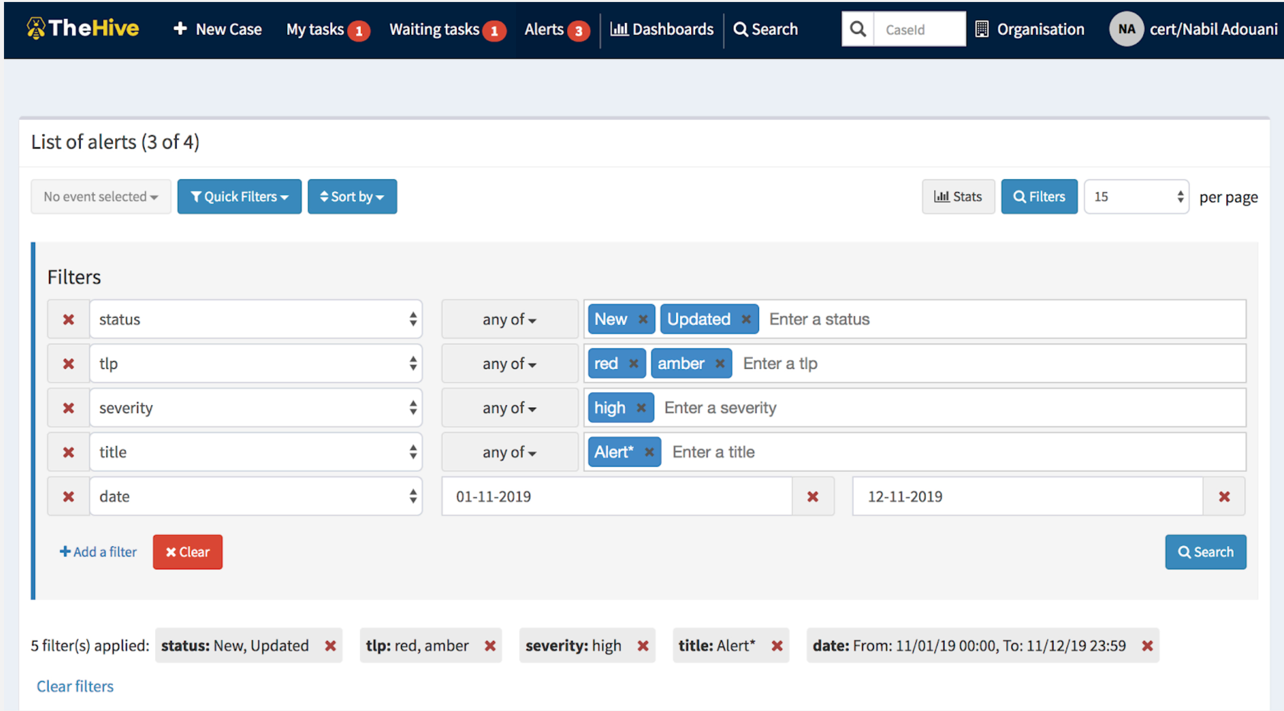


As a read-only user



UI Improvements

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



List of alerts (3 of 4)

Filters

✖	status	any of	New ✖ Updated ✖ Enter a status
✖	tlp	any of	red ✖ amber ✖ Enter a tlp
✖	severity	any of	high ✖ Enter a severity
✖	title	any of	Alert* ✖ Enter a title
✖	date	01-11-2019 ✖	12-11-2019 ✖

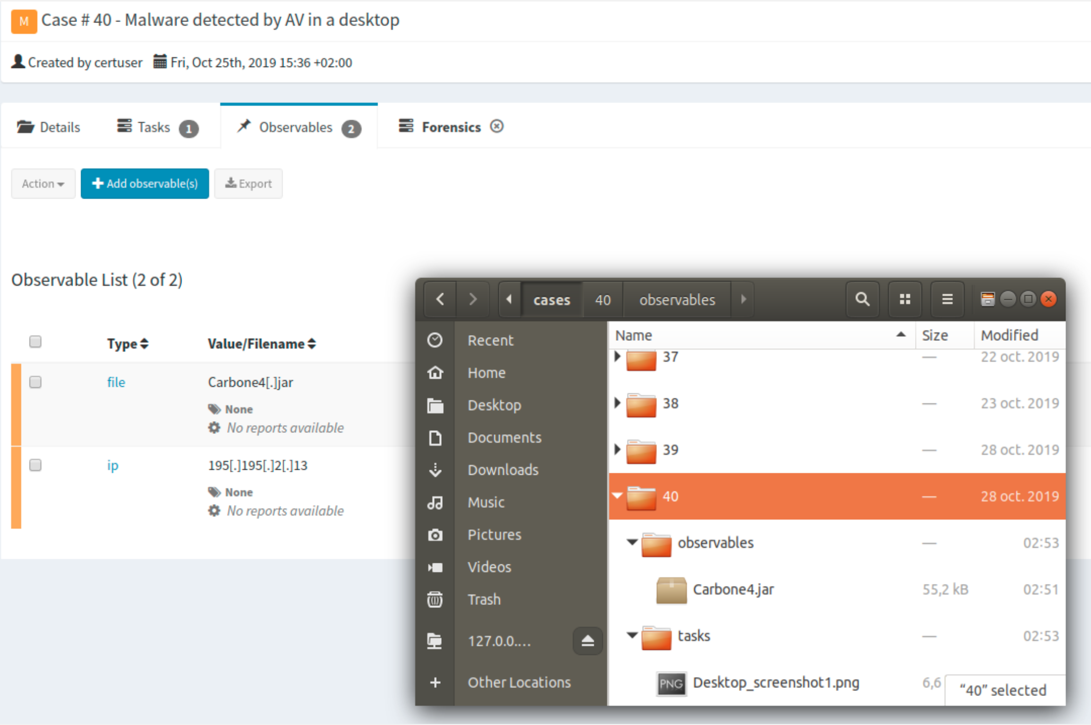
5 filter(s) applied: **status:** New, Updated ✖ **tlp:** red, amber ✖ **severity:** high ✖ **title:** Alert* ✖ **date:** From: 11/01/19 00:00, To: 11/12/19 23:59 ✖

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)



M Case # 40 - Malware detected by AV in a desktop

Created by certuser   Fri, Oct 25th, 2019 15:36 +02:00

Observable List (2 of 2)

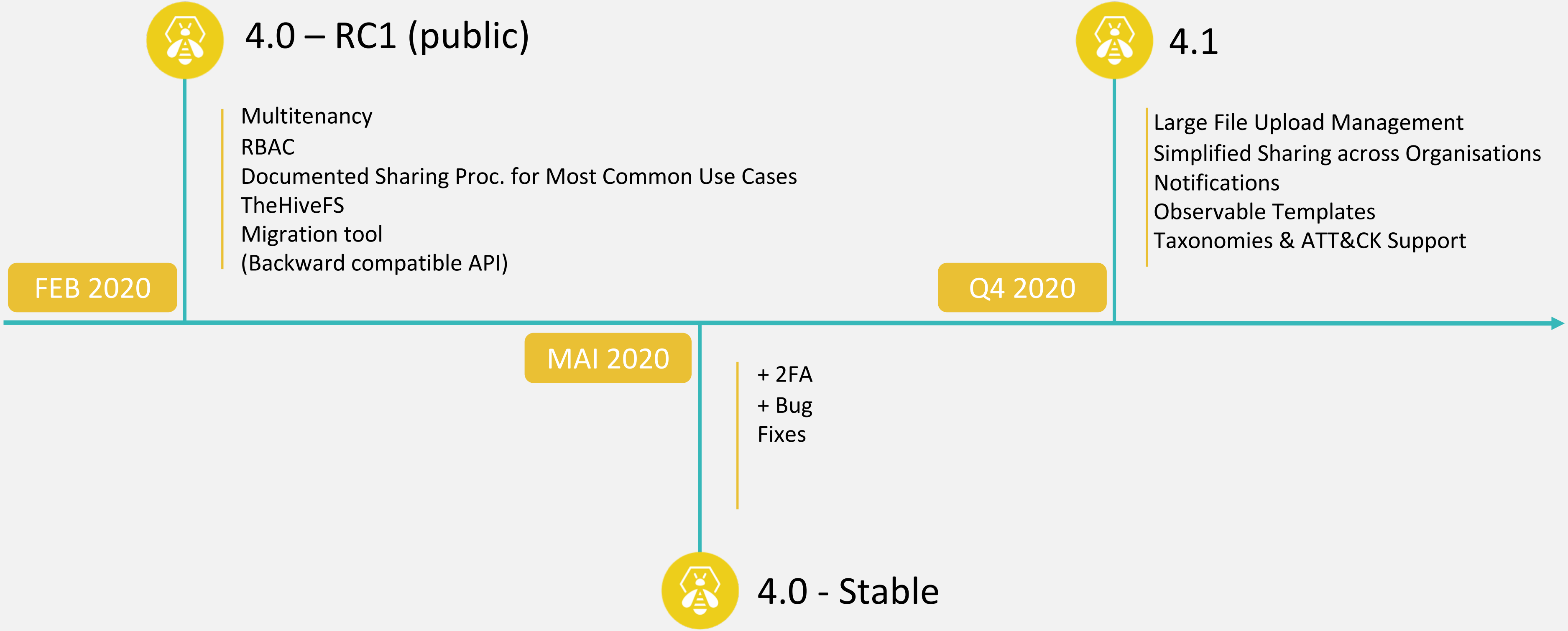
□	Type	Value/Filename
□	file	Carbone4[.]jar None *No reports available*
□	ip	195[.]195[.]2[.]13 None *No reports available*

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

Roadmap and future features

The Roadmap



FEB 2020

4.0 – RC1 (public)

Multitenancy
RBAC
Documented Sharing Proc. for Most Common Use Cases
TheHiveFS
Migration tool
(Backward compatible API)

MAI 2020

4.0 - Stable

+ 2FA
+ Bug
Fixes

Q4 2020

4.1

Large File Upload Management
Simplified Sharing across Organisations
Notifications
Observable Templates
Taxonomies & ATT&CK Support

StrangeBee

StrangeBee

Need Help?

Need assistance and support?

- StrangeBee is a company built by 3 TheHive cofounders to sustain the project
- It aims to answer the requests coming from a growing need for **support**, **professional services and advanced features**
- It offers:
  - Annual Support subscriptions
  - Professional Services
  - Training
- Need help? Send an email to **contact@strangebee.com**

StrangeBee

Thank You

Community

- https://blog.thehive-project.org
- https://gitter.im/TheHive-Project/TheHive
- https://twitter.com/TheHive_Project
- users@thehive-project.org

- https://www.strangebee.com
- contact@strangebee.com
- nabil@strangebee.com

StrangeBee