



TheHive 4

New features & Roadmap

Nabil Adouani

Co-founder of **TheHive** Project

@nadouani

@TheHive_Project

Copyright © StrangeBee. All rights reserved

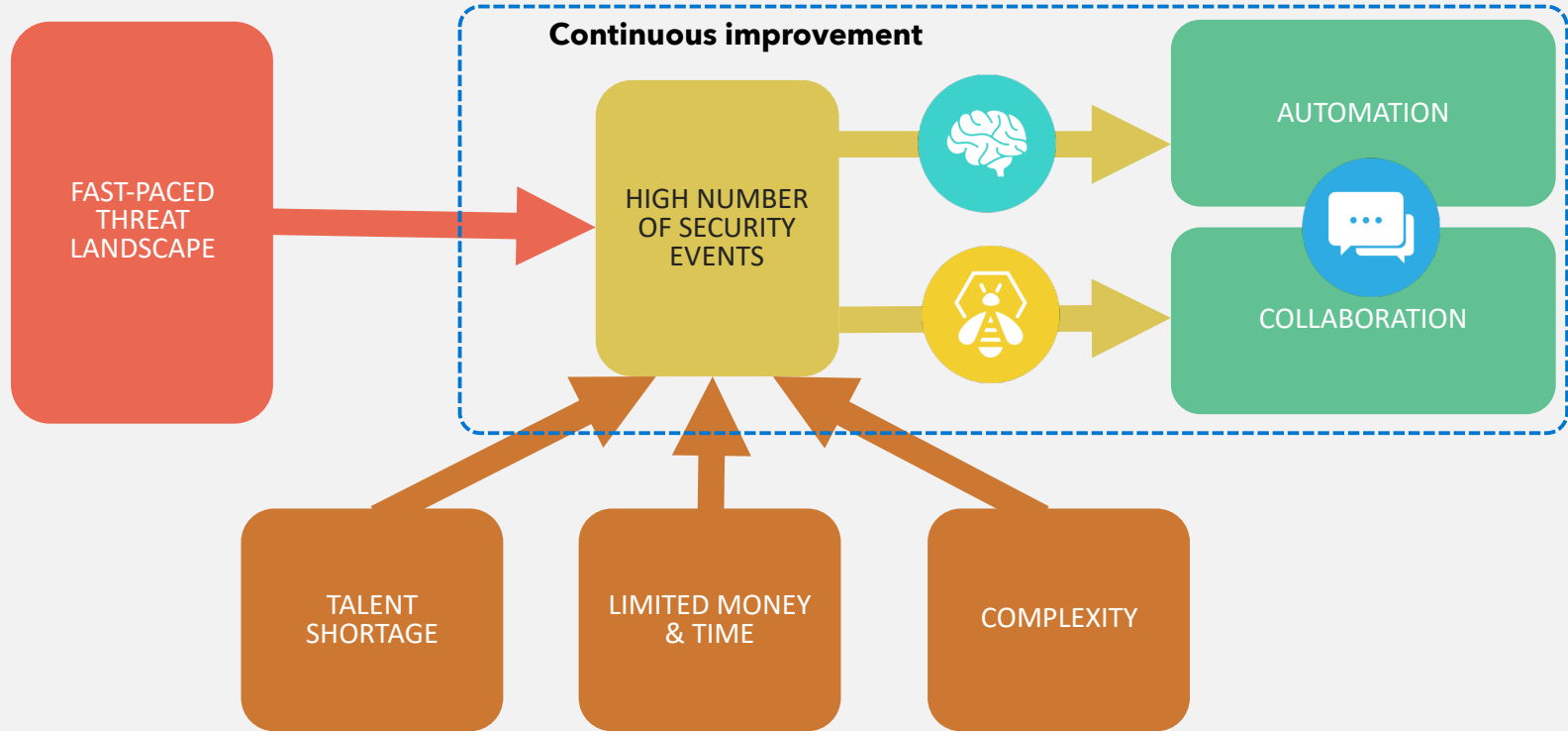
The Agenda

- 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



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**

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

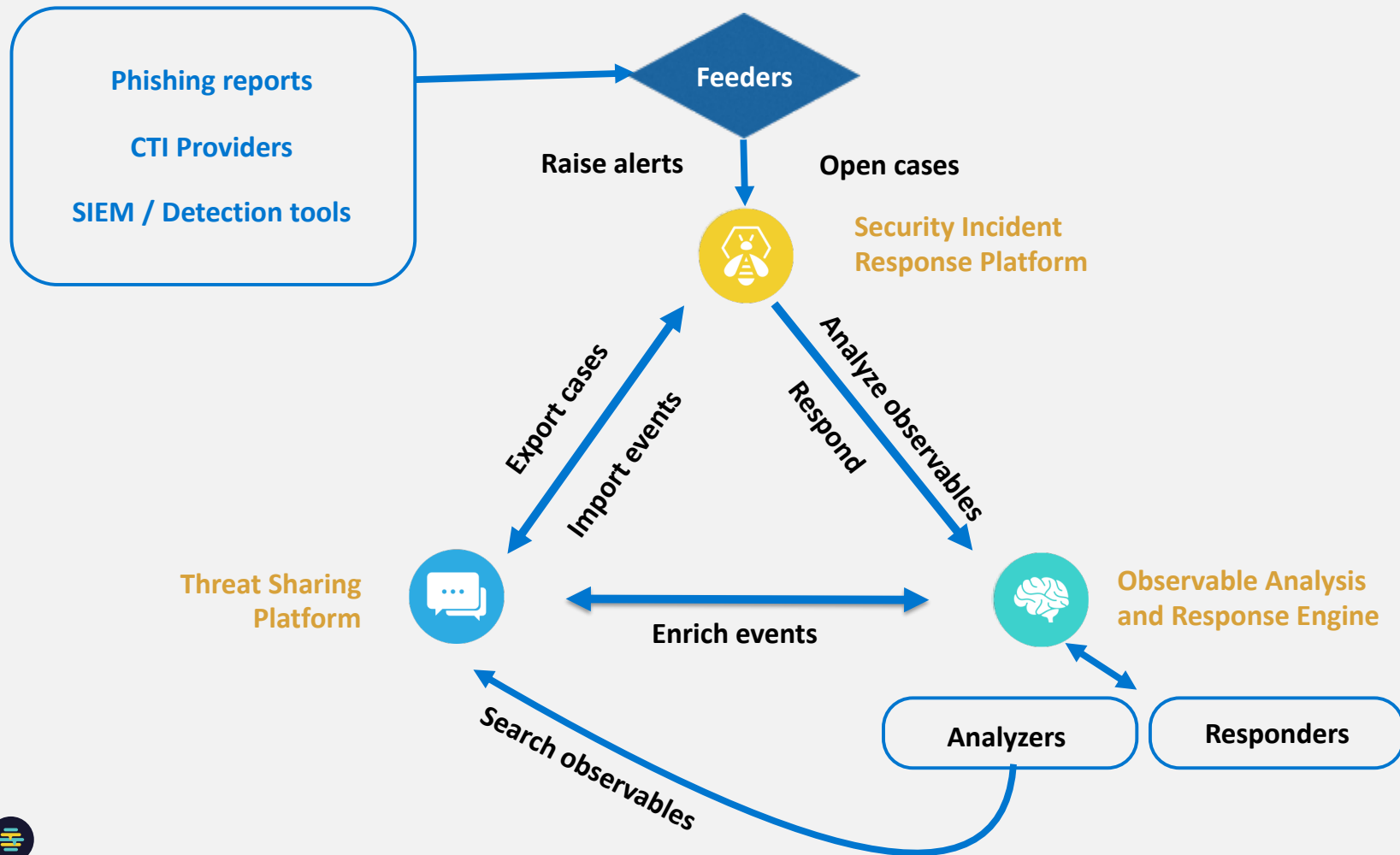
What's MISP ?



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



How do they work together?





TheHive, from 3 to 4

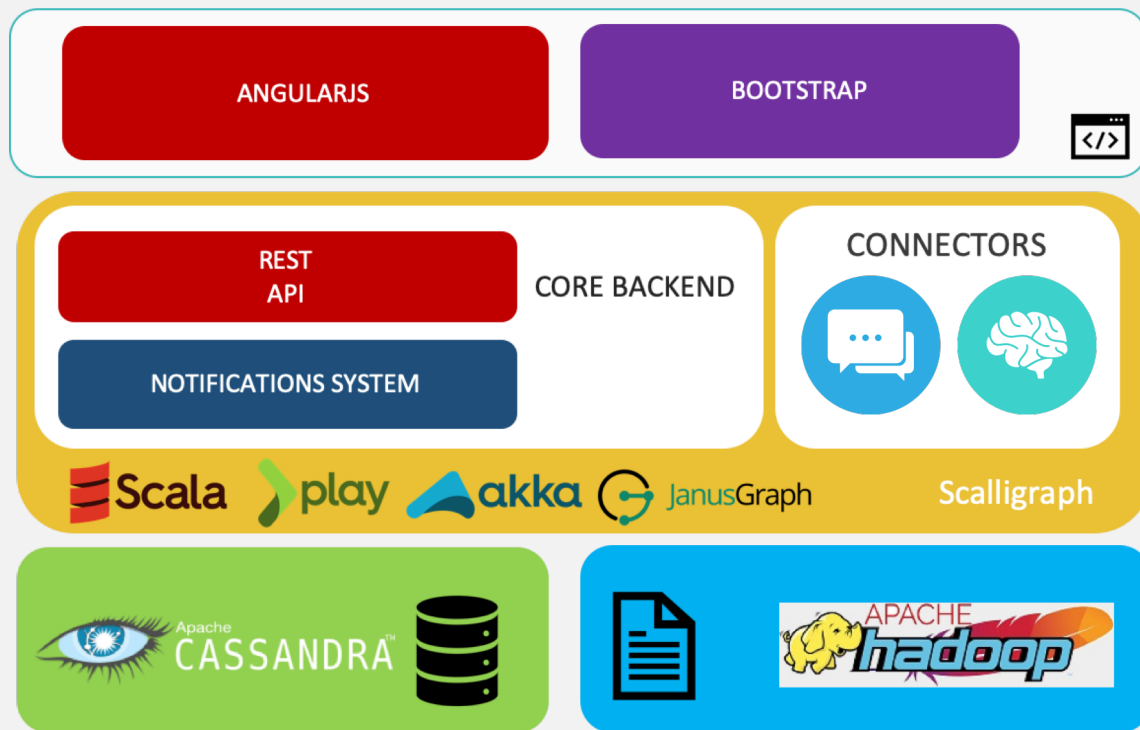
The Current Status

- 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

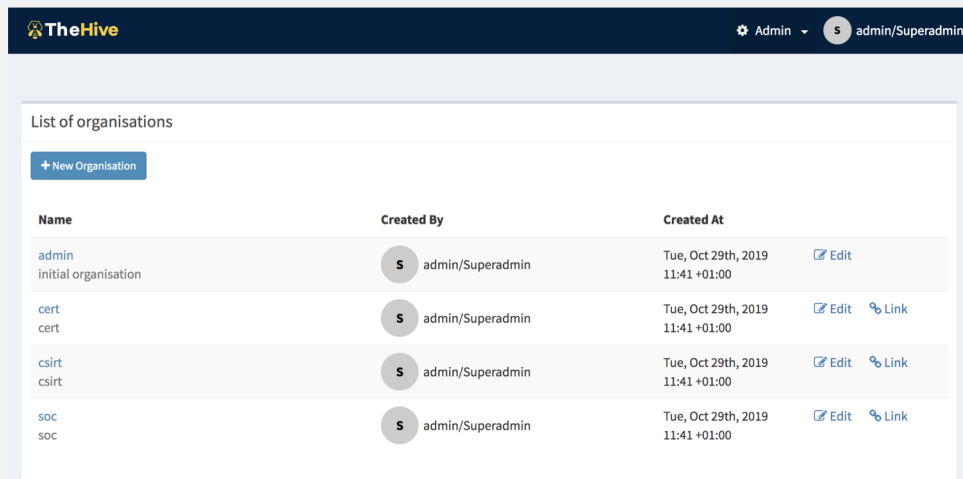
Data







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

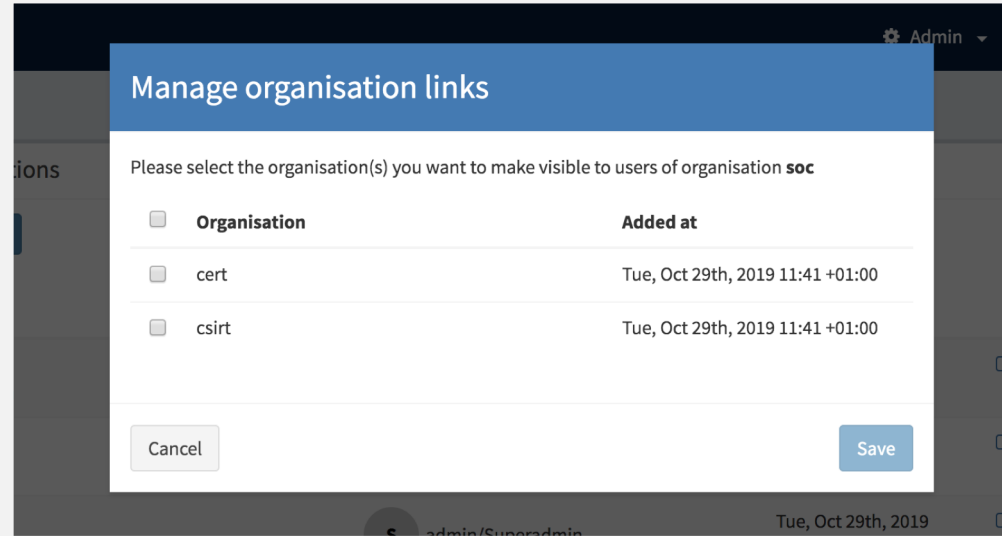


The screenshot shows the 'TheHive' web interface. At the top, there's a dark blue header with the 'TheHive' logo on the left and 'Admin' with a dropdown arrow and a user profile icon labeled 'admin/Superadmin' on the right. Below the header, the main content area is titled 'List of organisations'. There's a blue button with a plus icon and the text '+ New Organisation'. Below this is a table with three columns: 'Name', 'Created By', and 'Created At'. The table lists four organisations: 'admin' (initial organisation), 'cert' (cert), 'csirt' (csirt), and 'soc' (soc). Each row shows the organisation name, a user icon with the letter 'S' followed by 'admin/Superadmin', and the creation date and time 'Tue, Oct 29th, 2019 11:41 +01:00'. To the right of each row are two links: 'Edit' and 'Link'.

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

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



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	
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.**”
- Mechanism 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

 [+ New Case](#) [My tasks 1](#) [Waiting tasks 1](#) [Alerts 3](#) [Dashboards](#) [Search](#) [Organisation](#) [NA cert/Nabil Adouani](#)

M

Case # 33 - New Alert

+ Show live stream

Created by Nabil Adouani

Tue, Oct 29th, 2019 14:32 +01:00

1 alert

[Sharing](#) | [Close](#) | [Flag](#) | [Merge](#) | [Remove](#) | [Responders](#) v

[Details](#) | [Tasks 0](#) | [Observables 5](#) | [Sharing](#) v

Action v

[+ Add observable\(s\)](#)


[Export](#)

[Stats](#)

[Filters](#)

15

per page



StrangeBee

20

Collaboration and Sharing - Cases

The screenshot displays the 'TheHive' web interface. A modal window titled 'Share case' is open, allowing the user to share Case # 32 - [MISP]Sample 2. The modal contains the following fields:

- Organisation ***: A list box with 'soc' selected.
- Profile ***: A dropdown menu with 'incident-handler' selected.
- Tasks ***: A dropdown menu with 'all' selected.
- Observables ***: A dropdown menu with 'none' selected.

At the bottom of the modal are 'Cancel' and 'Save' buttons. The background interface shows the case details for Case # 32 - [MISP]Sample 2, created by Nabil Adouani on Tue, Oct 29th, 2019 12:00. It includes tabs for Details, Tasks (2), and Observables, and a table of shared cases.

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

Collaboration and Sharing - Tasks

The screenshot shows the TheHive web interface. A modal dialog titled "Select organisations" is open in the center. The dialog has a table with two columns: "Organisation" and "Profile". There is one row with "soc" in the Organisation column and "incident-handler" in the Profile column. At the bottom of the dialog are "Cancel" and "Save" buttons. The background is a task details page for a task assigned to "Nabil Adouani" with a status of "InProgress". The page includes sections for "Basic Information", "Description" (marked as "Not specified"), "Task logs" (with an "Add new task log" button and a "Sort by: Newest first" dropdown), and "Task sharing" (with an "Add share" button). At the bottom, there is a table for task sharing records.

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

Collaboration and Sharing - Observables

The screenshot displays the TheHive web application interface. A modal dialog titled "Select organisations" is open, allowing the user to choose an organization for collaboration. The dialog contains a table with two columns: "Organisation" and "Profile".

Organisation	Profile
<input checked="" type="checkbox"/> csirt	incident-handler
<input type="checkbox"/> soc	incident-handler

At the bottom of the modal, there are "Cancel" and "Save" buttons. The background interface shows a sidebar with navigation options like "Hash", "Date added", "Is IOC", "Has been sighted", "Tags", "Description", "Analysis", "Analyzer", and "Sharing". The main content area is currently empty, displaying "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

The screenshot displays the TheHive web interface. The top navigation bar includes the TheHive logo, a '+ New Case' button, and links for 'My tasks' (1), 'Waiting tasks' (1), 'Alerts' (3), 'Dashboards', 'Search', 'Organisation', and a user profile for 'cert/Nabil Adouani'. The main content area is titled 'List of alerts (3 of 4)'. It features a toolbar with 'No event selected', 'Quick Filters', 'Sort by', 'Stats', 'Filters', and a '15 per page' dropdown. Below this is a 'Filters' section with five rows of filterable attributes: 'status' (New, Updated), 'tlp' (red, amber), 'severity' (high), 'title' (Alert*), and 'date' (01-11-2019 to 12-11-2019). Each filter row has a dropdown menu, a 'any of' selector, and a text input field. At the bottom, a summary bar shows '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'. A 'Clear filters' link is also present.

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 displays the TheHive web interface for Case #40, titled "Malware detected by AV in a desktop". The interface includes tabs for Details, Tasks, Observables, and Forensics. Below these tabs is an "Observable List (2 of 2)" table with columns for Type and Value/Filename.

Type	Value/Filename
file	Carbone4[.]jar <small>None No reports available</small>
ip	195[.]195[.]12[.]13 <small>None No reports available</small>

Overlaid on the right is a macOS-style file explorer window showing the "cases" directory. The "observables" folder is selected, displaying its contents: "37", "38", "39", "40", "observables", "Carbone4.jar", "tasks", and "Desktop_screenshot1.png". The "40" folder is highlighted, and a status bar at the bottom indicates "40" selected.



Roadmap and future features

The Roadmap



4.0 – RC1 (public)

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

FEB 2020

MAY 2020

- + 2FA
- + Bug Fixes



4.0 - Stable



4.1

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

Q4 2020



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**

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

