TLP:WHITE

OWASP COPENHAGEN MEETUP 2021

THE BEST PARTNER IN CRIME OF YOUR SIEM

Nabil Adouani

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

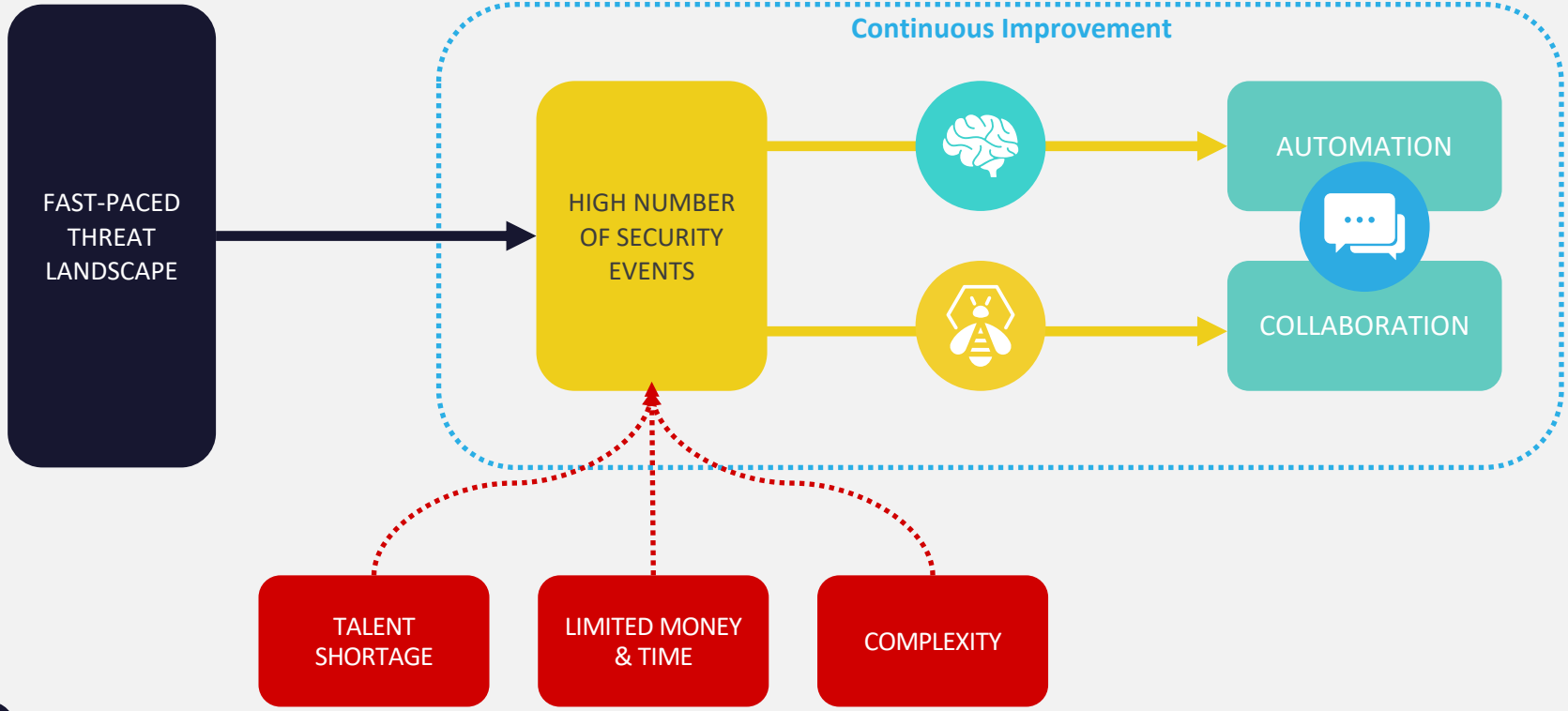
StrangeBee

The Agenda

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

StrangeBee

Drive Down The Time to React

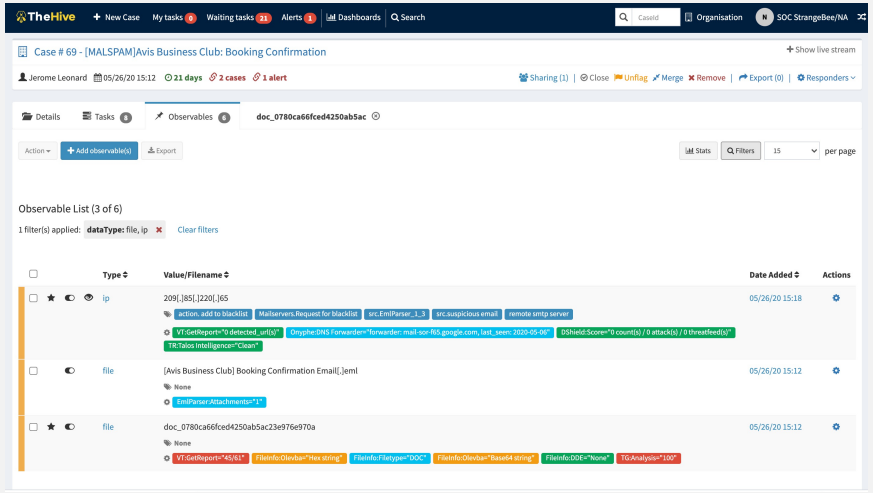


StrangeBee

The Products

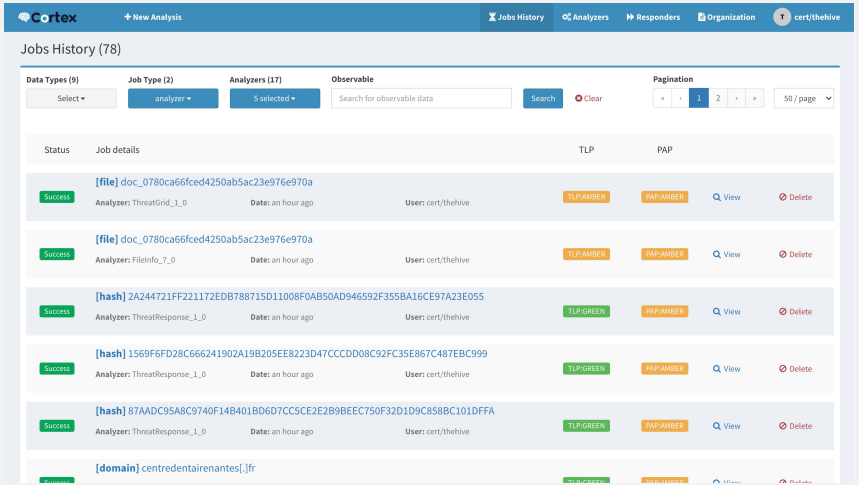
TheHive

Security Incident Response



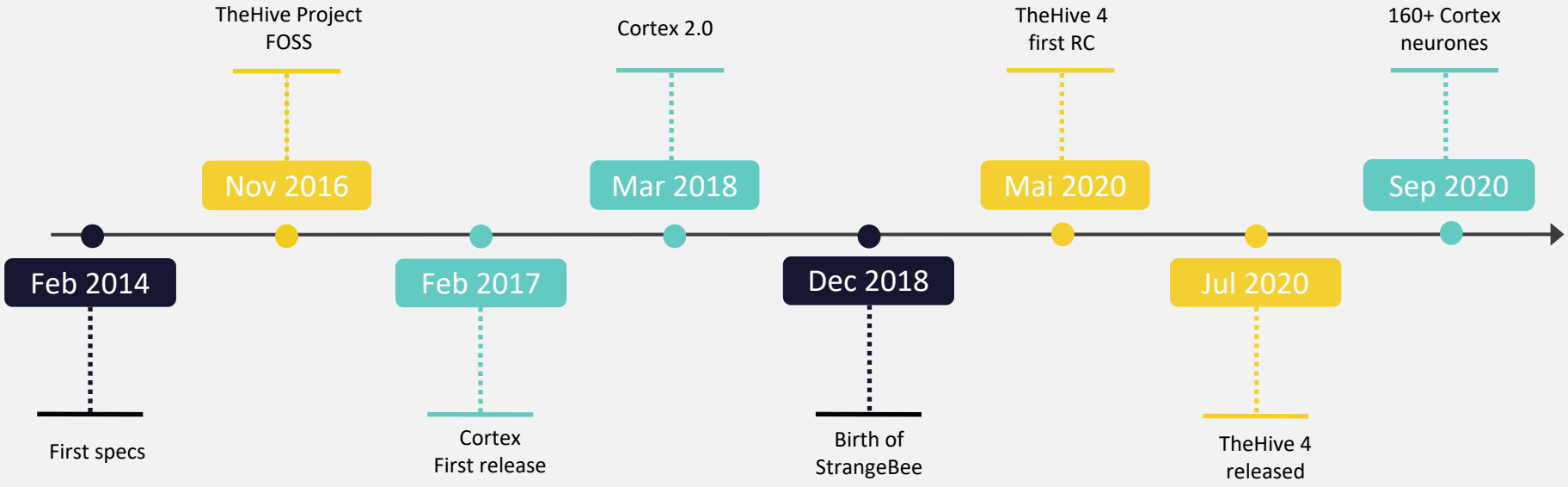
Cortex

Observable Analysis and Active Response



StrangeBee

The Timeline



StrangeBee

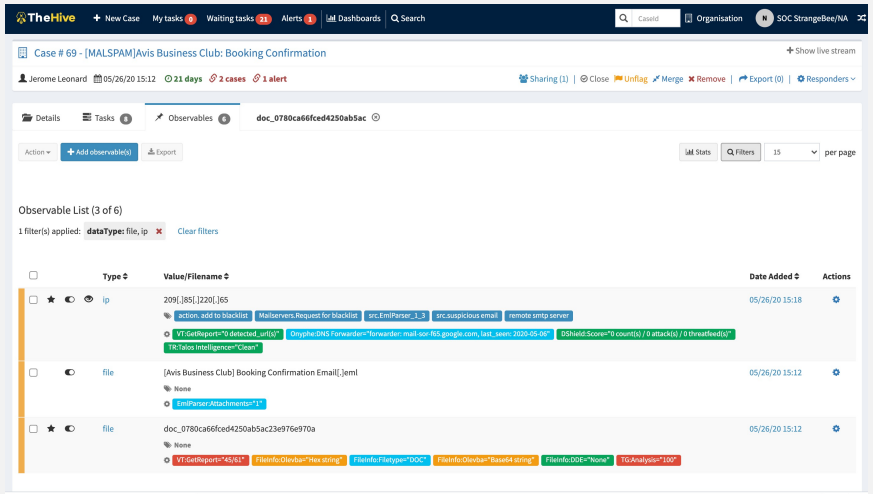
TheHive & Cortex Overview

StrangeBee

TheHive overview

TheHive

Security Incident Response Platform



- **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)

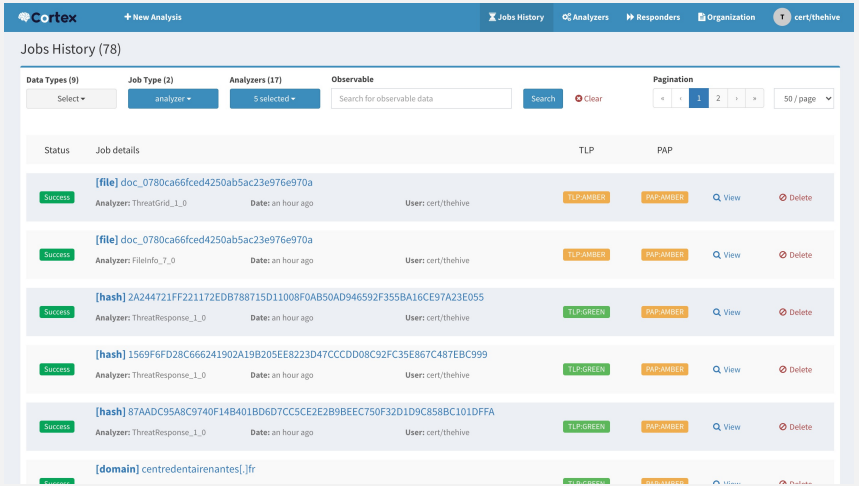
StrangeBee

Cortex overview

- **Define** libraries of analyzers and responders (3rd 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

Cortex

Observable Analysis and Active Response Platform



StrangeBee

Terminology

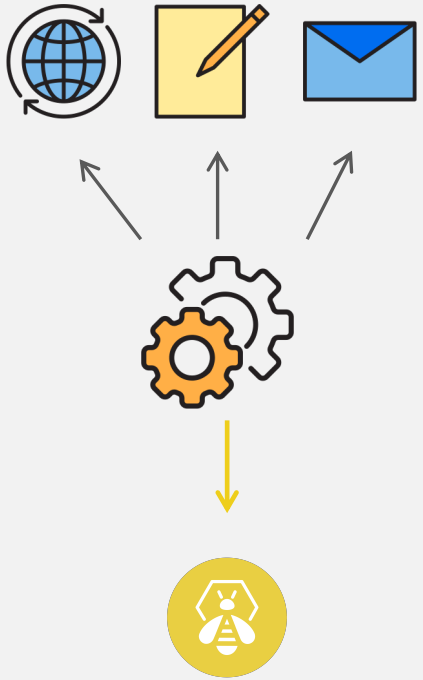
Feeders, Analyzers and Responders

StrangeBee

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

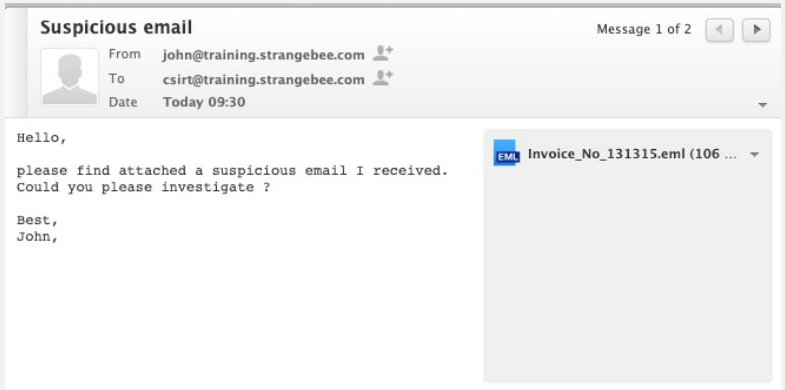
- Python Client Library – TheHive4py

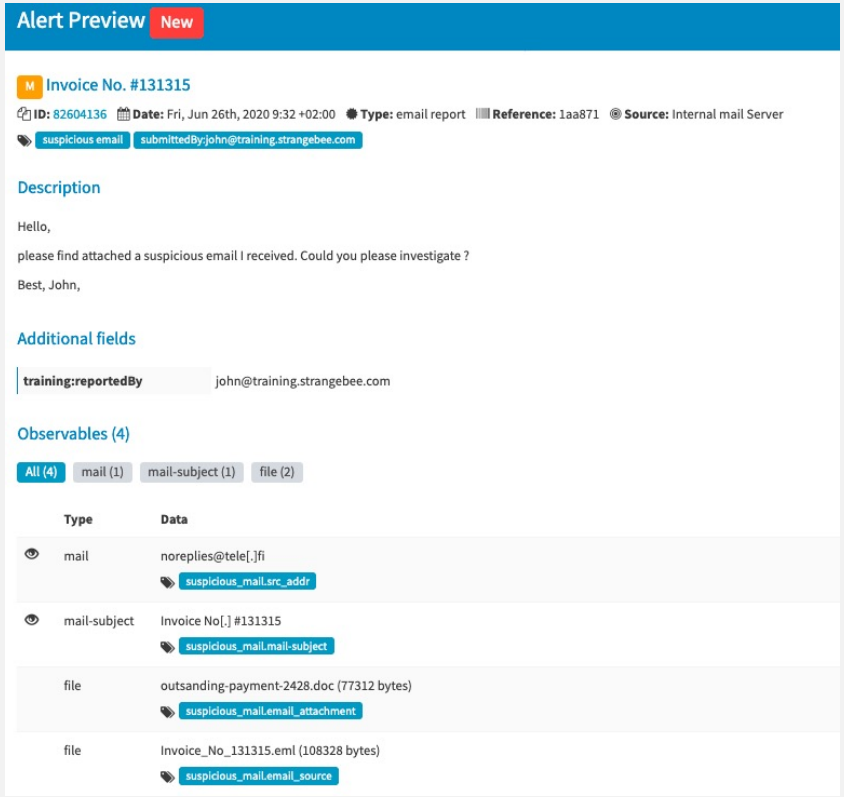


StrangeBee

Feeders

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

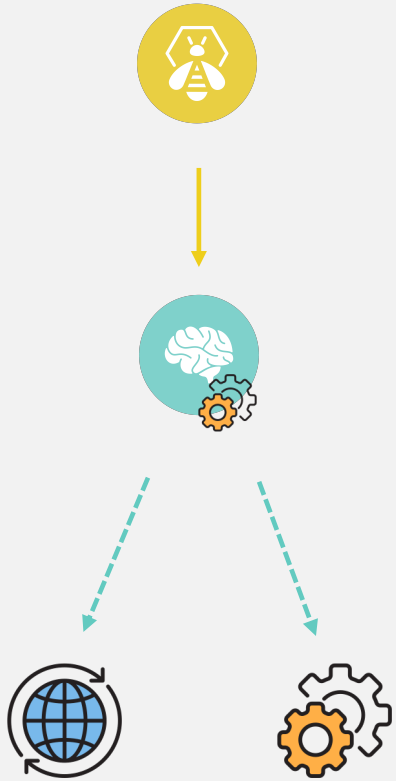




StrangeBee

Analyzers

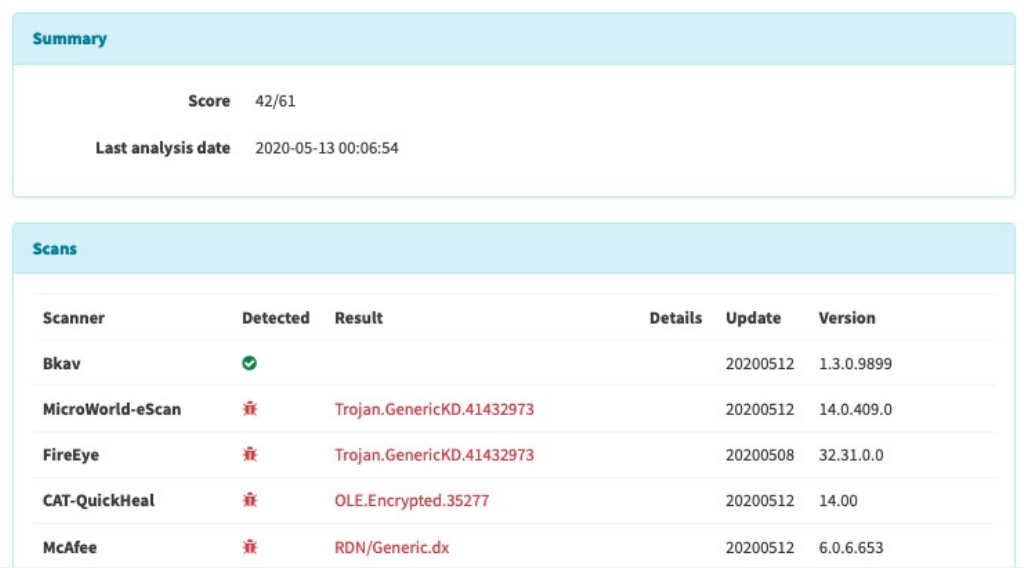
- **Process** one (1) *Observable*
- **Deliver** an analysis report
  - Query external services
  - CTI, IP/Domain repurtation, Sandboxes…
- **Input**: Observable metadata and configuration
- **Output:** Summary report + Long report + Observables *(optional)*



StrangeBee

Analyzers

- Example*: Get VirusTotal report from a Hash file*



Summary

Score	42/61
Last analysis date	2020-05-13 00:06:54

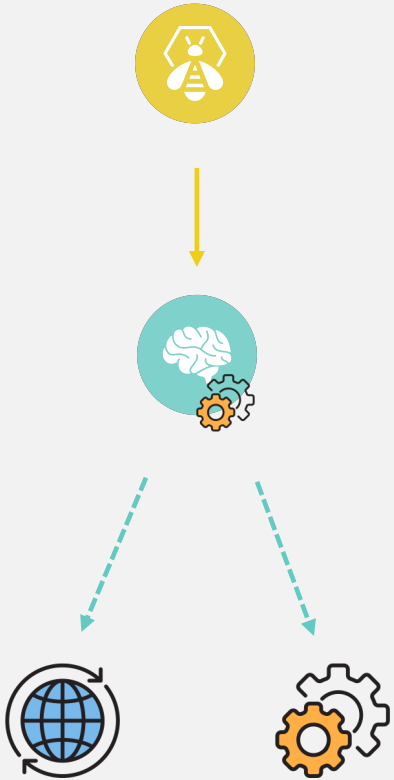
Scans

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

StrangeBee

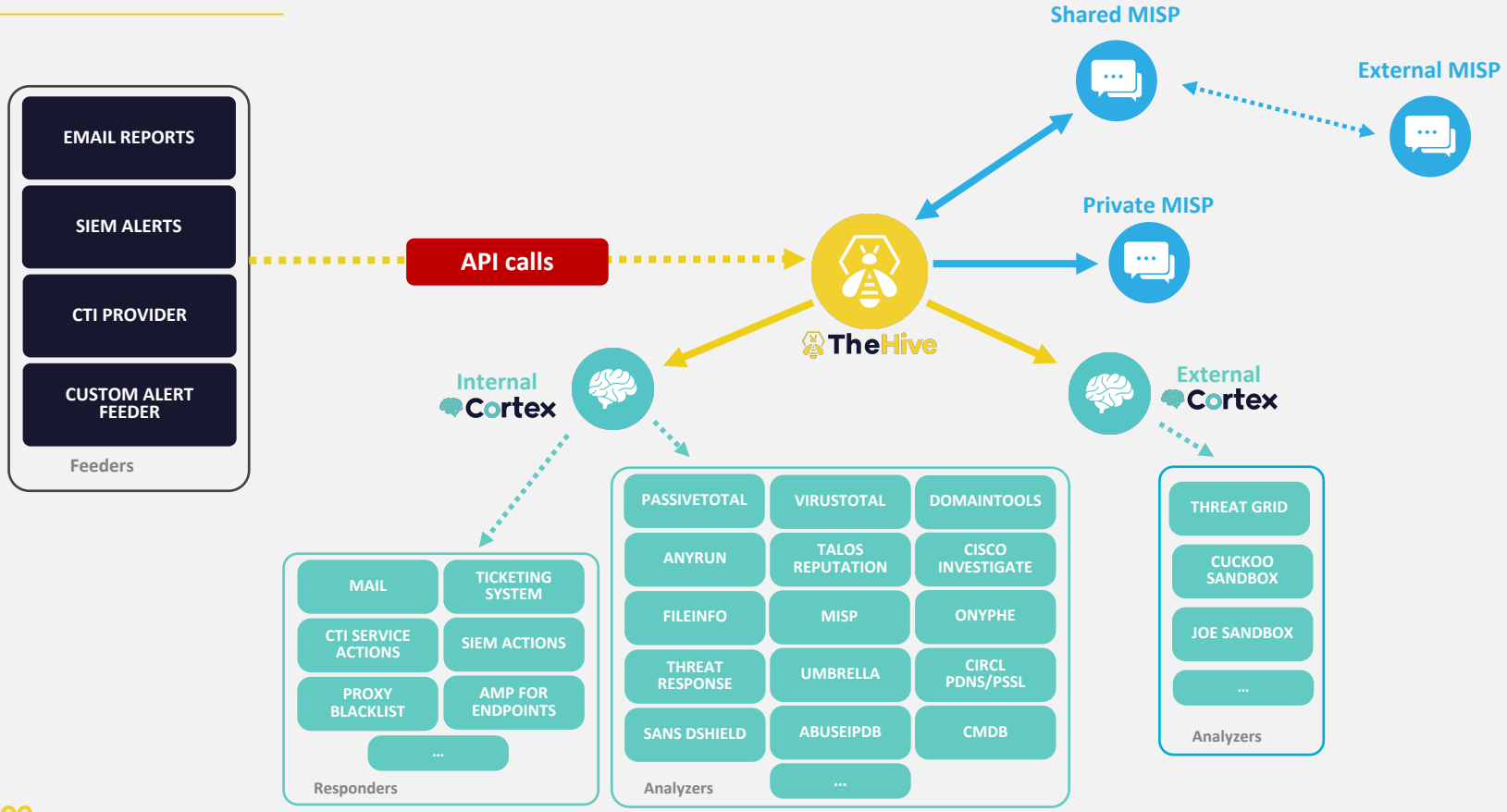
Responders

- **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 »



StrangeBee

Typical Integration



StrangeBee

TheHive and SIEMs

StrangeBee

TheHive & SIEMs

64%

Of our users, integrate TheHive with a SIEM

StrangeBee

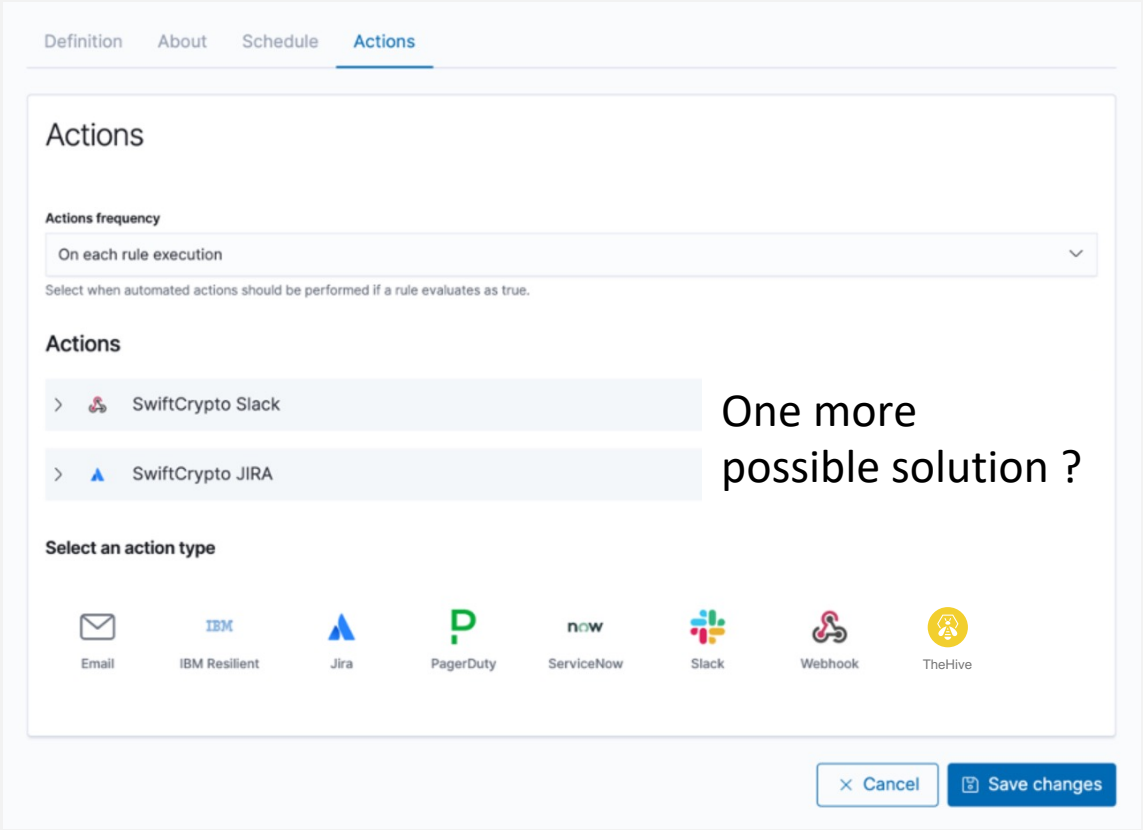
TheHive & Elastic Stack

- TheHive 3 and Cortex use Elasticsearch
- ELK is one of the most used SIEMs with TheHive
- Thanks to Elasatlert and its "**HIVE**" connector

  "Easy & Flexible Alerting With ElasticSearch"

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

TheHive & Elastic Stack

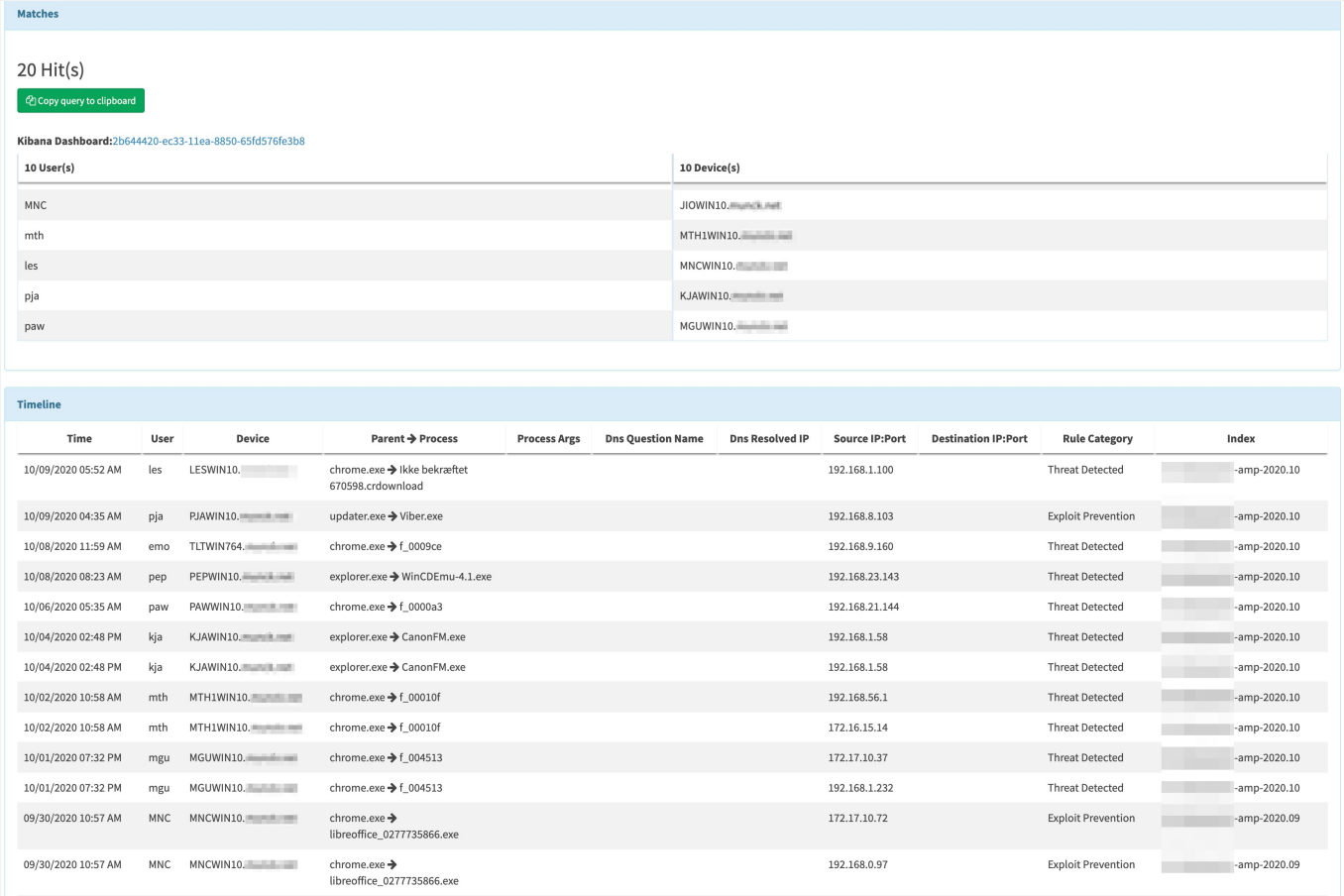


One more possible solution ?

StrangeBee

TheHive & Elastic Stack

- Cortex has an ES analyzer, by Nick Prokop



Matches

20 Hit(s)

Copy query to clipboard

Kibana Dashboard: 2b644420-ec33-11ea-8850-65fd576fe3b8

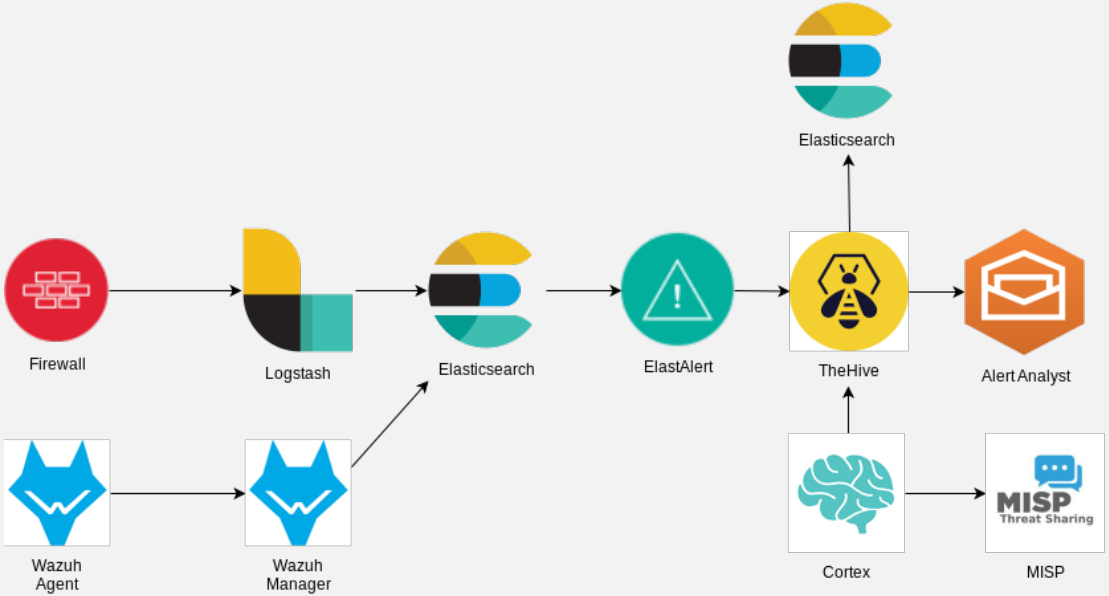
10 User(s)	10 Device(s)
MNC	JIOWIN10.
mth	MTH1WIN10.
les	MNCWIN10.
pja	KJAWIN10.
paw	MGUWIN10.

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 bekræftet 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

StrangeBee

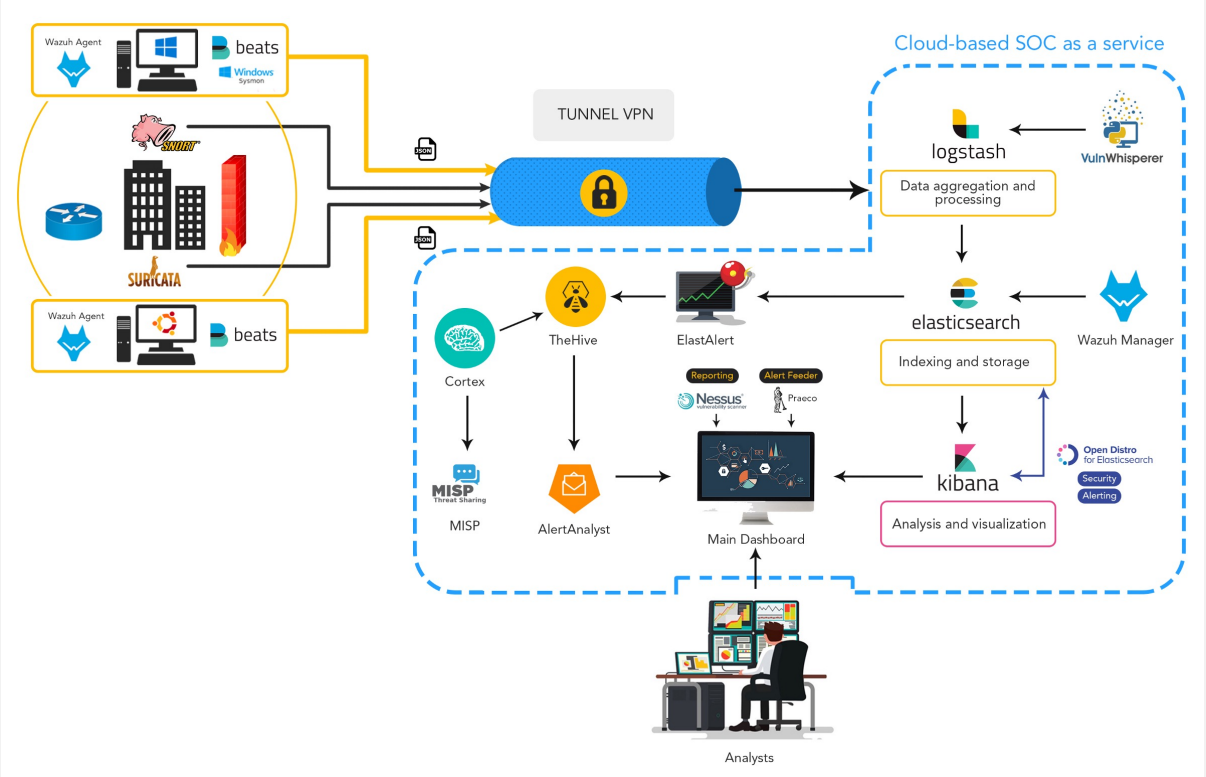
TheHive & Elastic Stack - Examples



Open Source SIRP with Elasticsearch and TheHive

StrangeBee

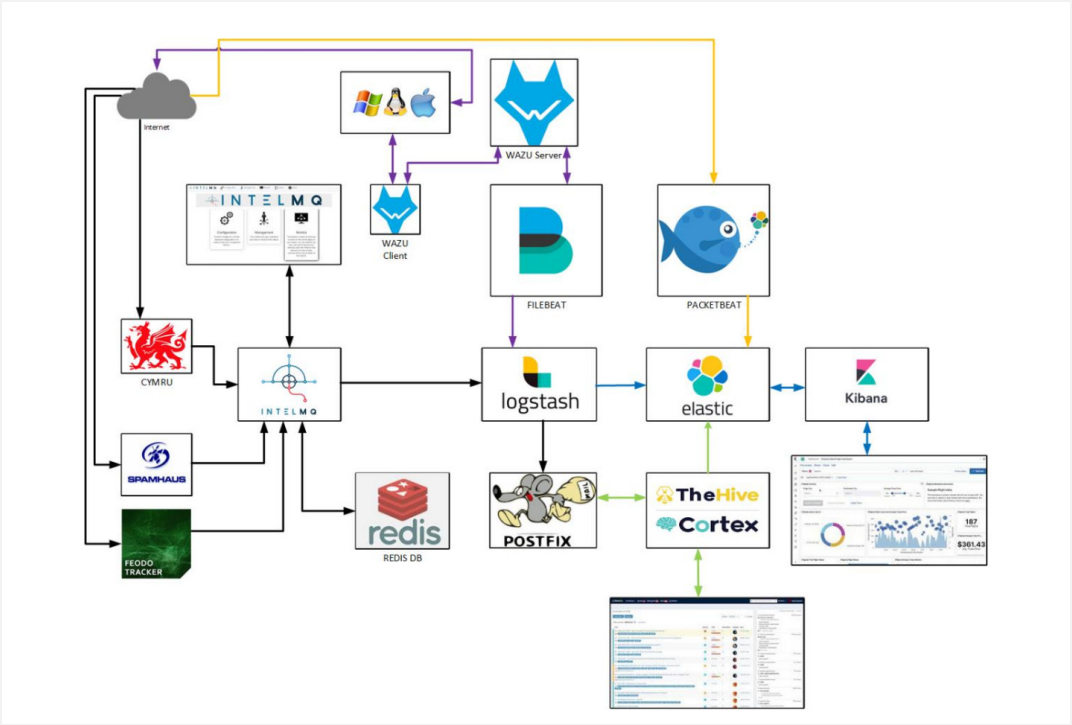
TheHive & Elastic Stack - Examples



Deploying of infrastructure and technologies for a SOC as a Service (SOCasS)

StrangeBee

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)

StrangeBee

TheHive & Elastic Stack – Bundles

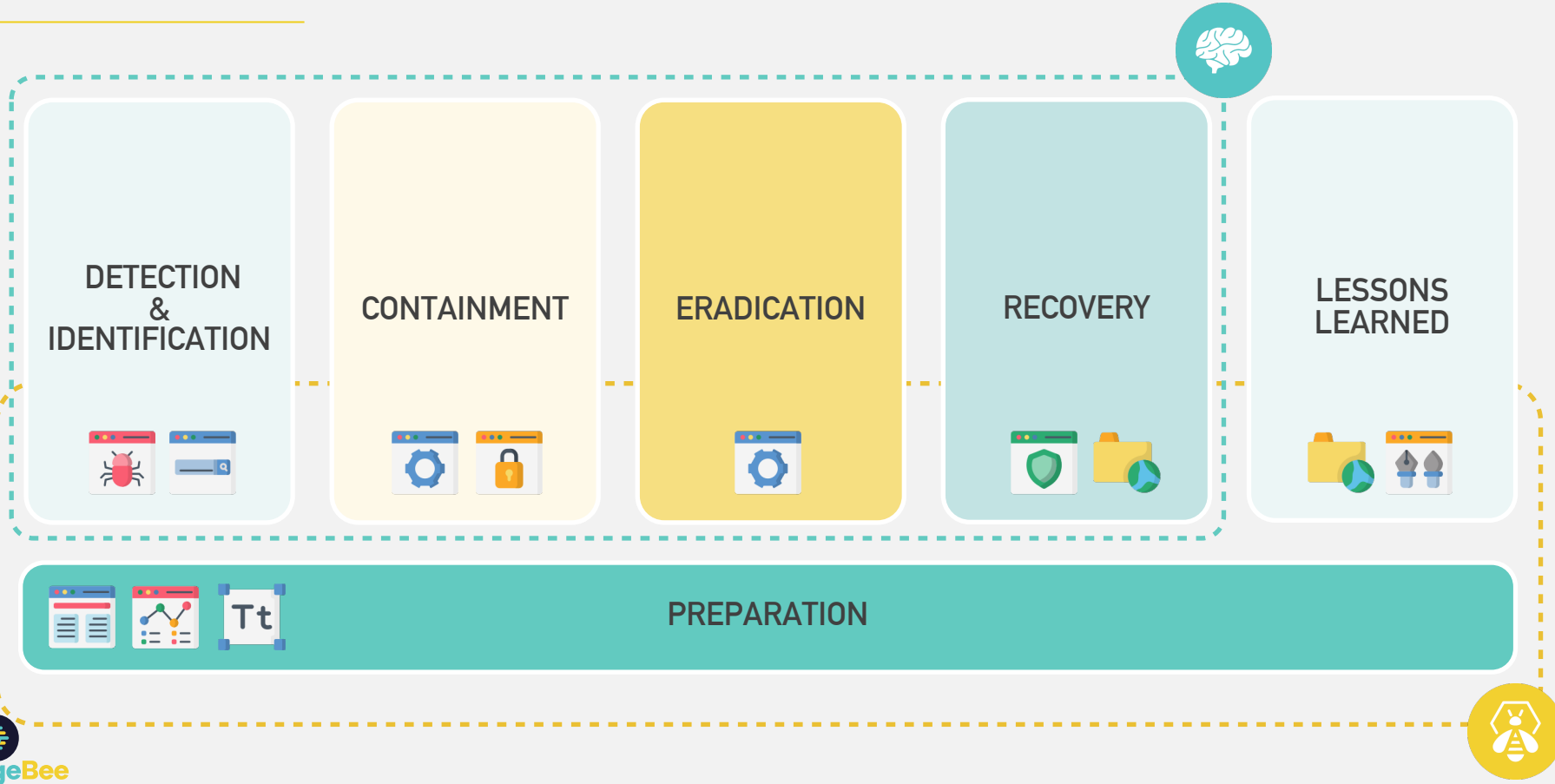
- Many projects include TheHive, Cortex and ELK as a bundled package:

StrangeBee

Incident Response using TheHive & Cortex

StrangeBee

Incident Response Process



StrangeBee

TheHive 4 features

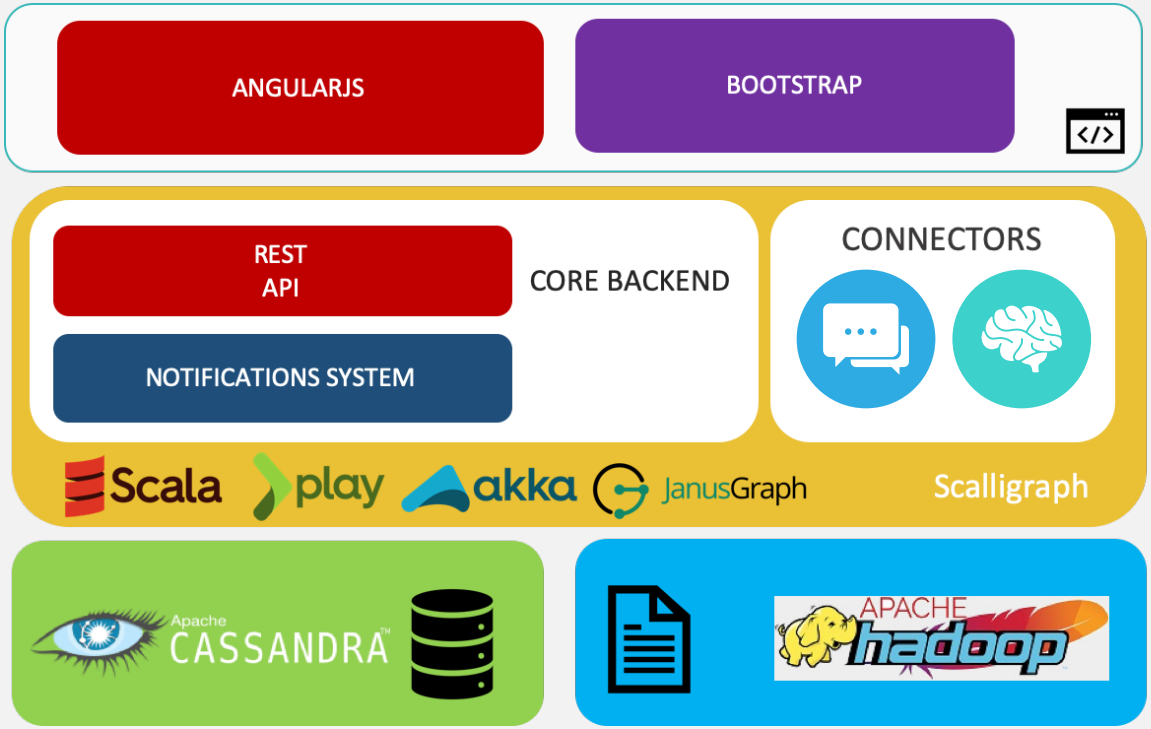
StrangeBee

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

StrangeBee

The Architecture



Front end

TheHive core application

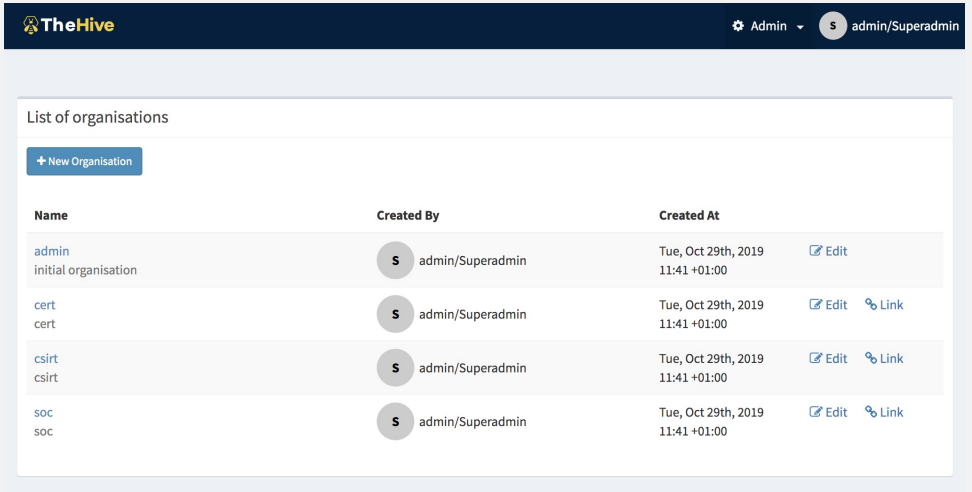
Data

A deep look into the new features

StrangeBee

Welcome to Organisations

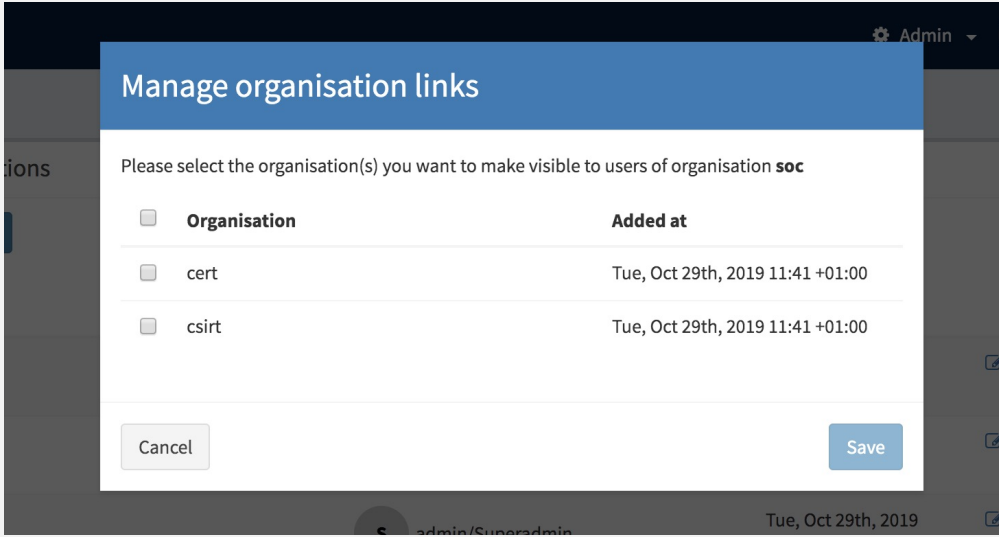
- An organisation
  - Contains one or several users
  - Defines what its users can do, can see (permissions)
- Organisation data is by default isolated
  - Creates logic isolation of data
  - An org can't access data that's not tied to it
- A user can belong to one or several organisations



StrangeBee

Organisation Visibility

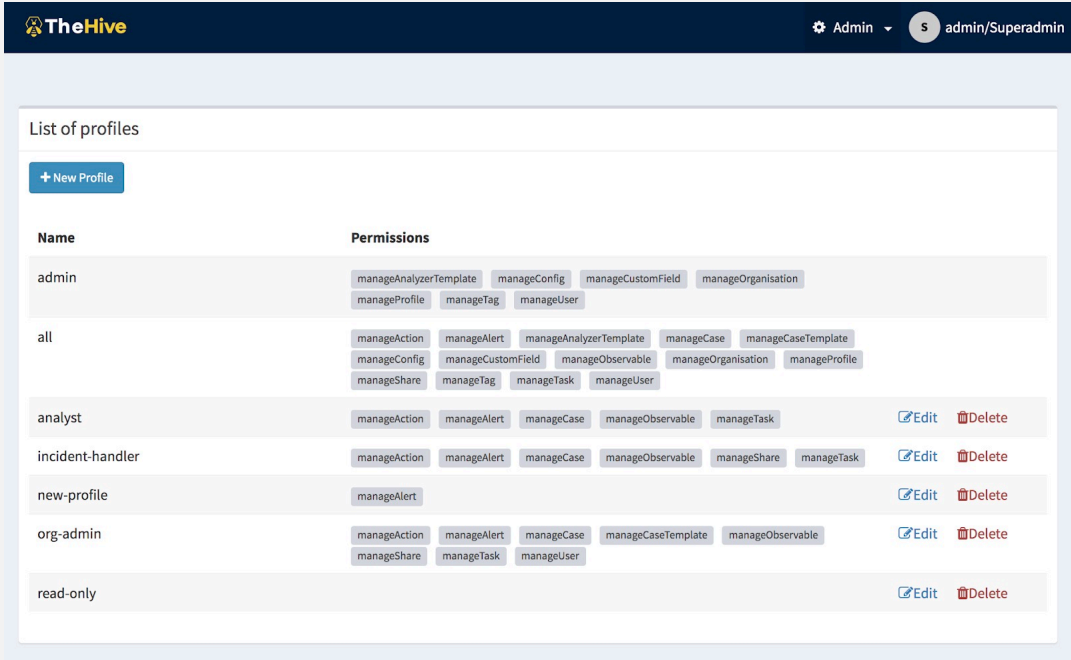
- Super administrators can define which organisation can collaborate with which one
- An organisation must be ‘linked’ to other organisations to be able to share data (cases/tasks) with them
- ‘linking’ is a temporary term



StrangeBee

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*



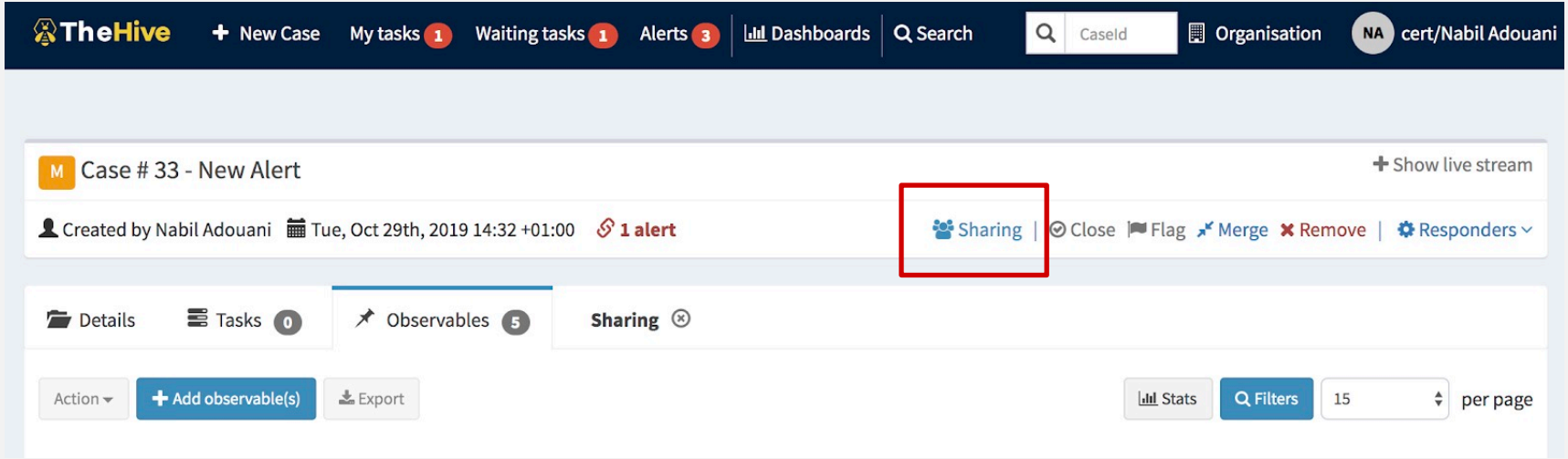
StrangeBee

Collaboration and Sharing

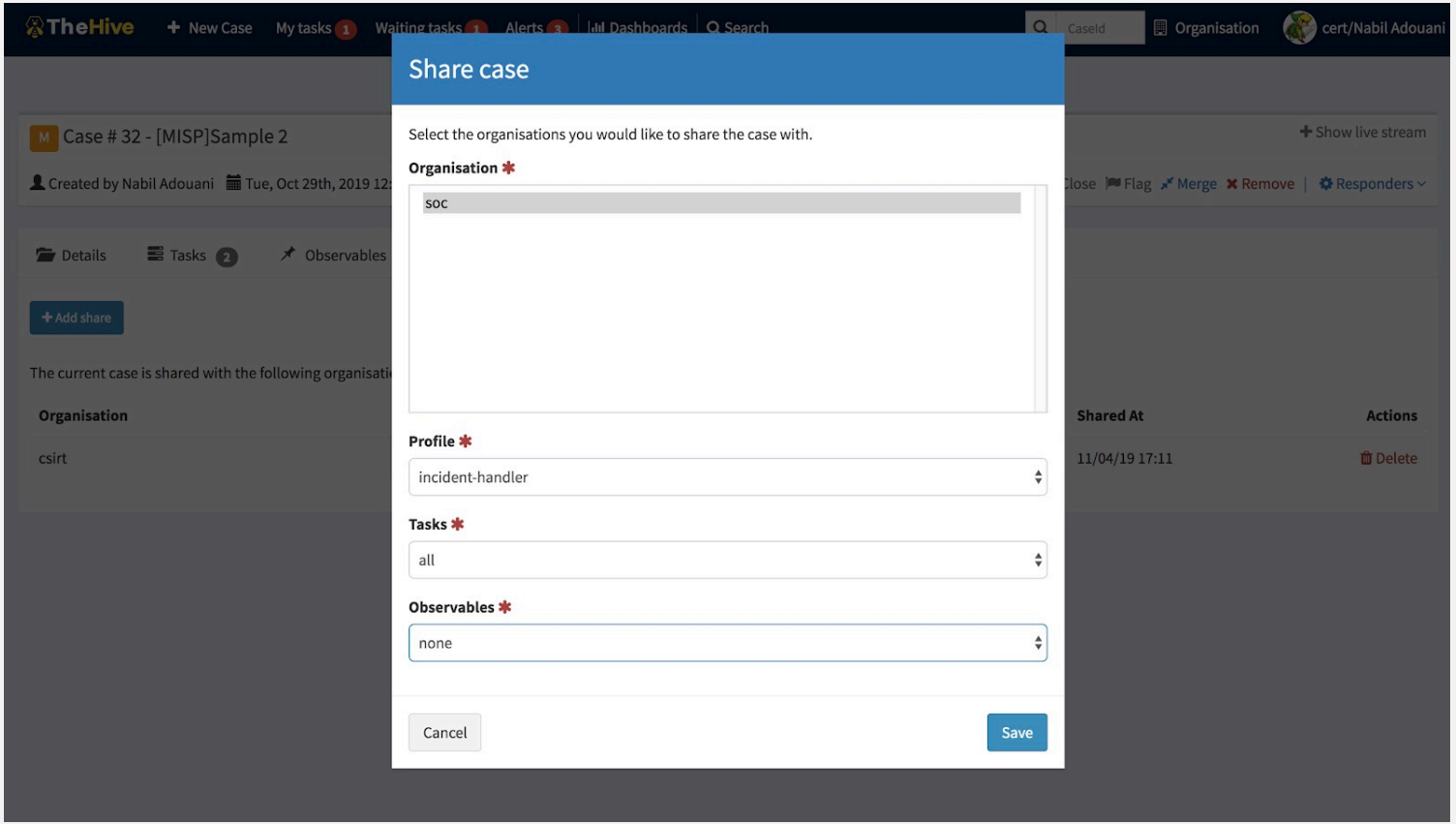
- Sharing = “Make an object **I own**, **visible** by an Organisation **I trust**.”
- Mecanism that allows two or more organisations to collaborate
- Sharing is possible for Cases, Tasks and Observables
- Requires *manageShare* permission
- For Cases, there is a dedicated tab in case details page
- For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

StrangeBee

Collaboration and Sharing - Cases



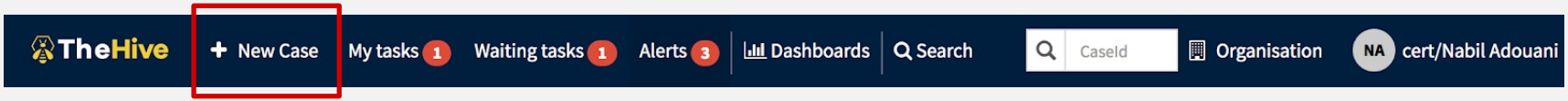
Collaboration and Sharing - Cases



UI Improvements

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

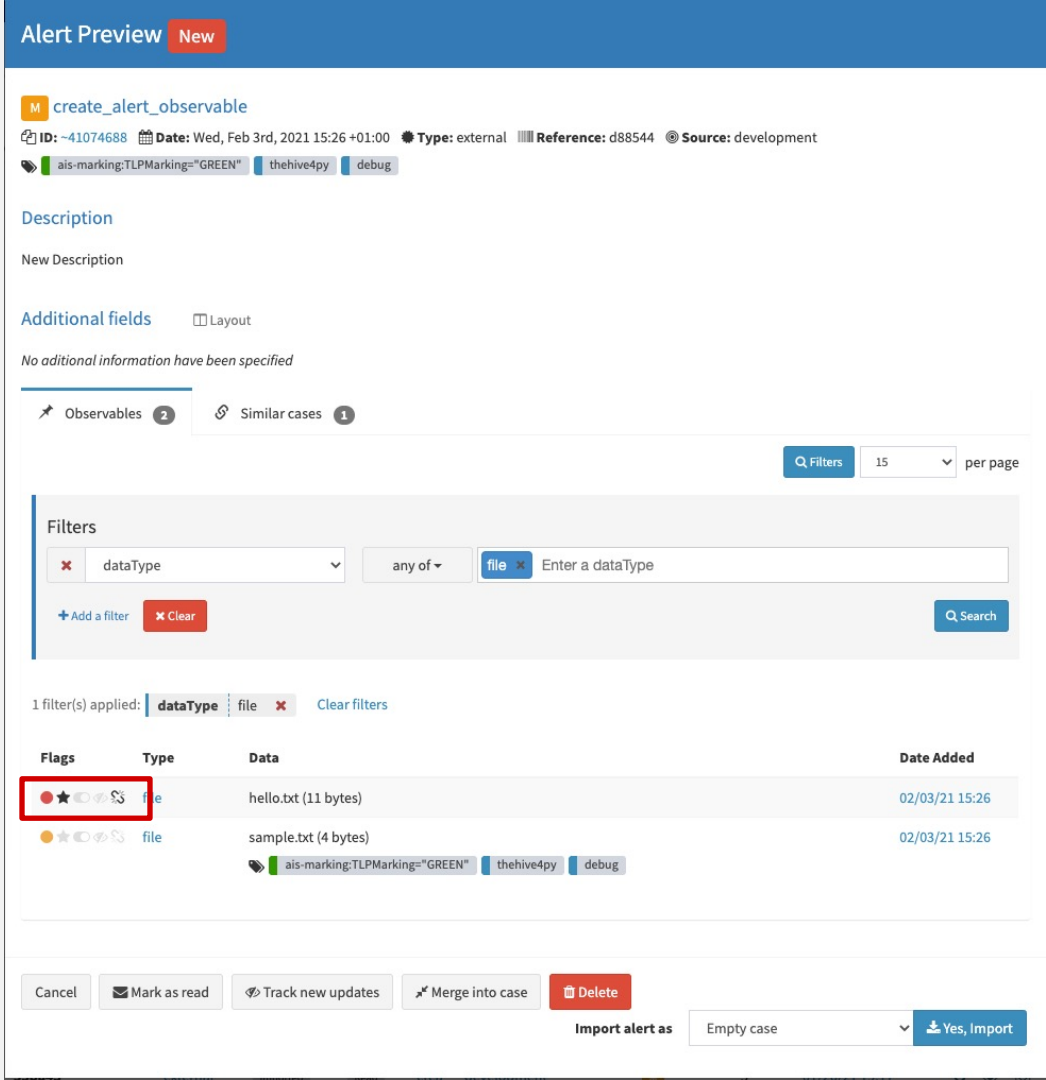
As an organisation administrator



As a read-only user

Enhanced Alert Triage

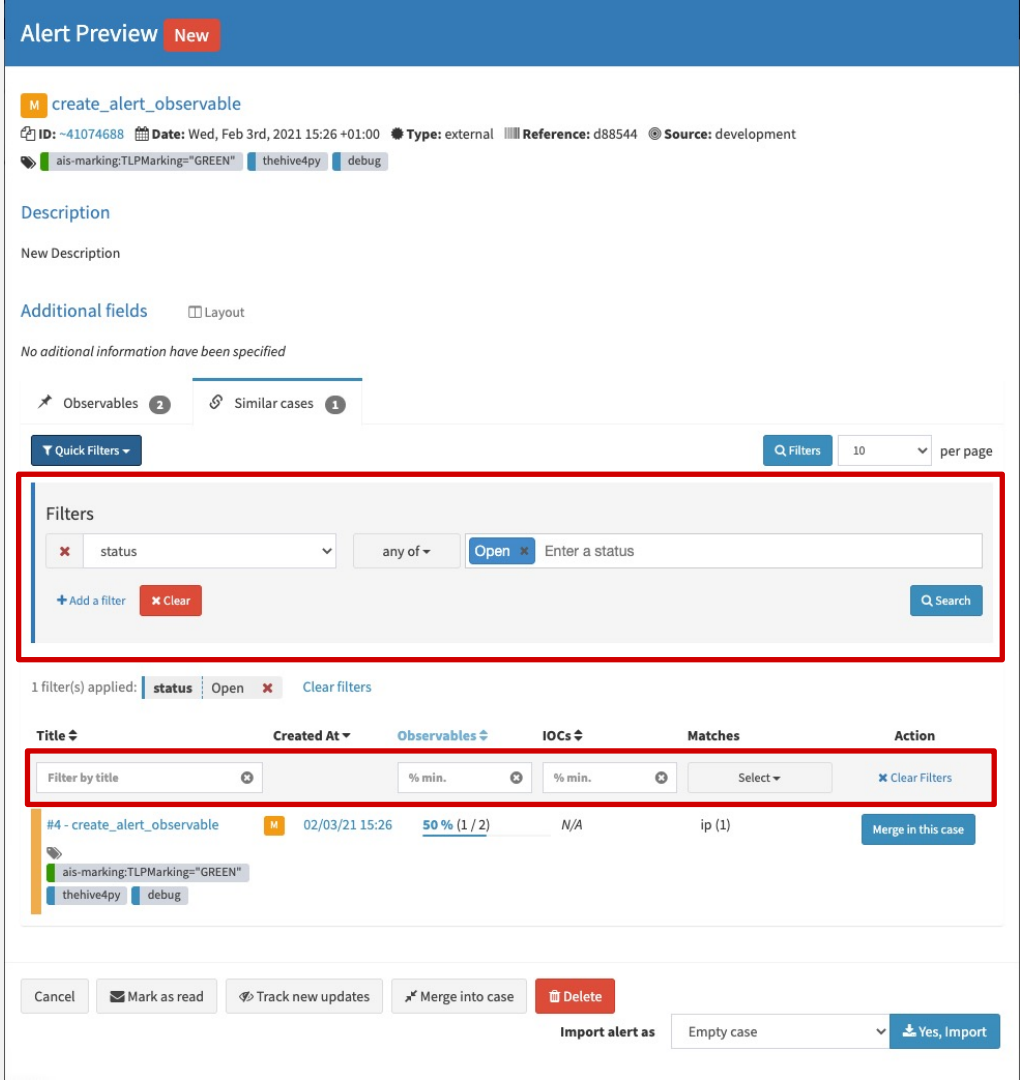
- Reviewed Alert observables section: pagination + filters + performance
- Support for *ignoreSimilarity* flag observables



StrangeBee

Enhanced Alert Triage

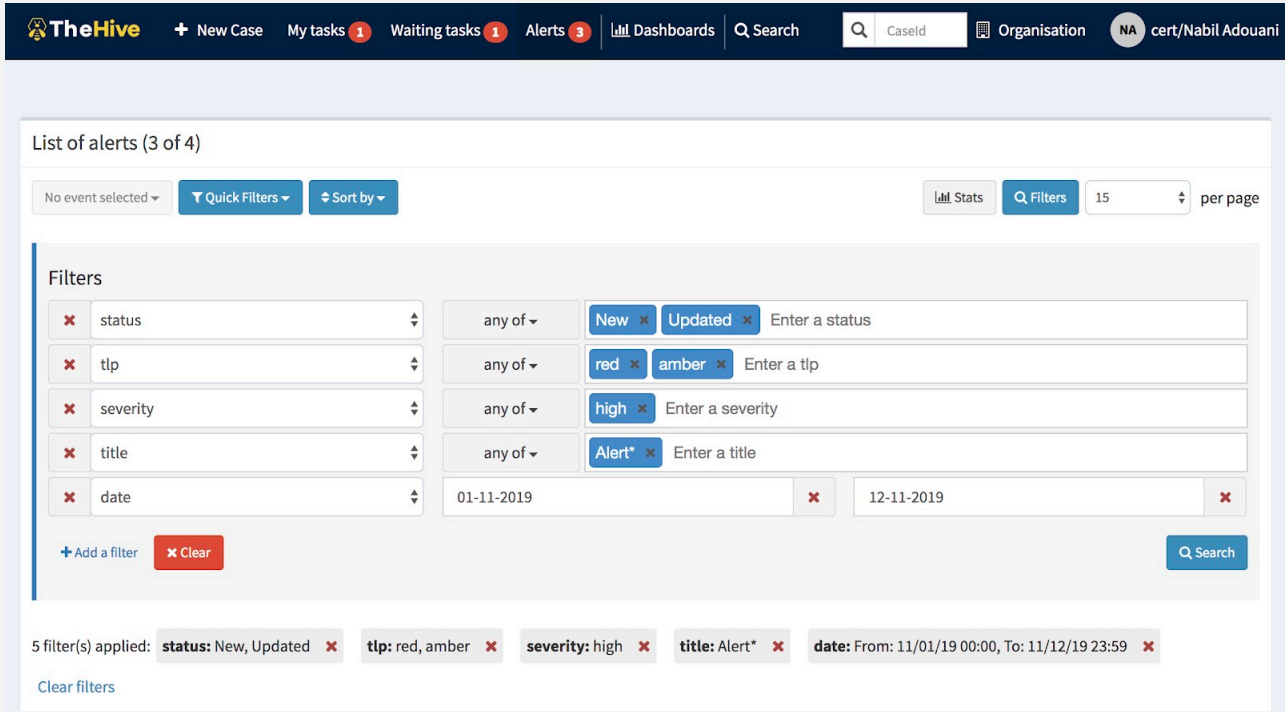
- Reviewed Alert similar cases section:
  - Pagination
  - Filters
  - Matched observable types
- Support for *ignoreSimilarity* flag observables



StrangeBee

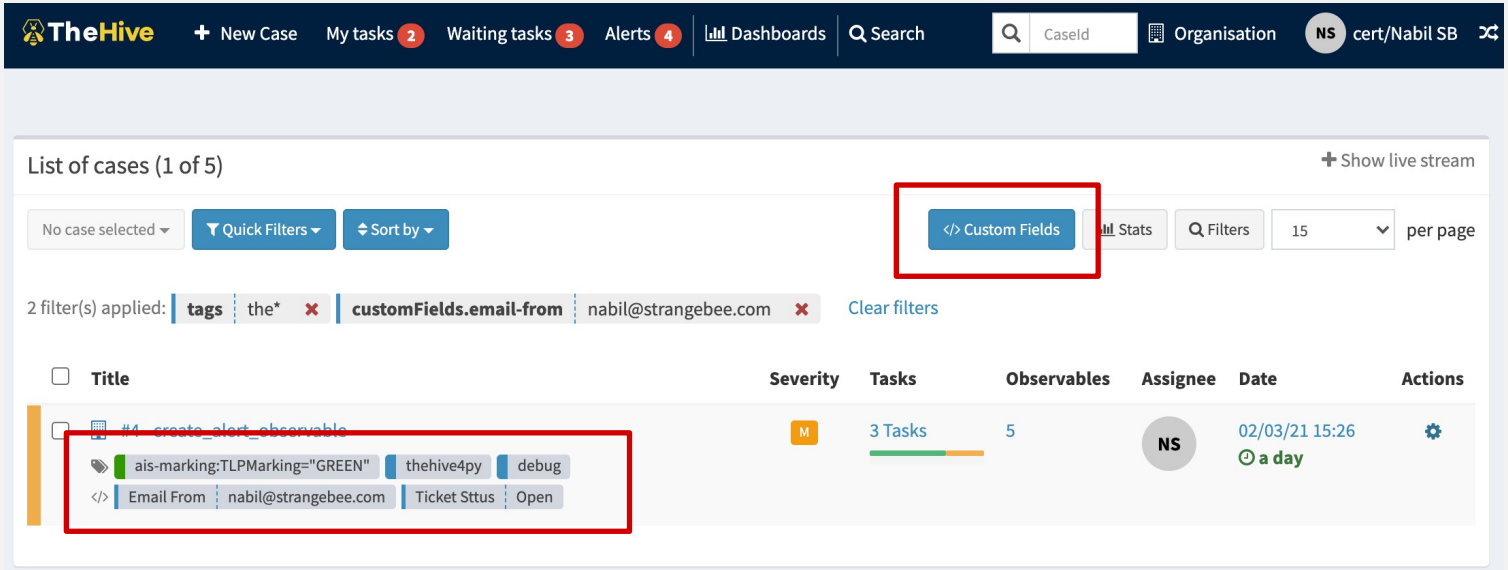
UI Improvements

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



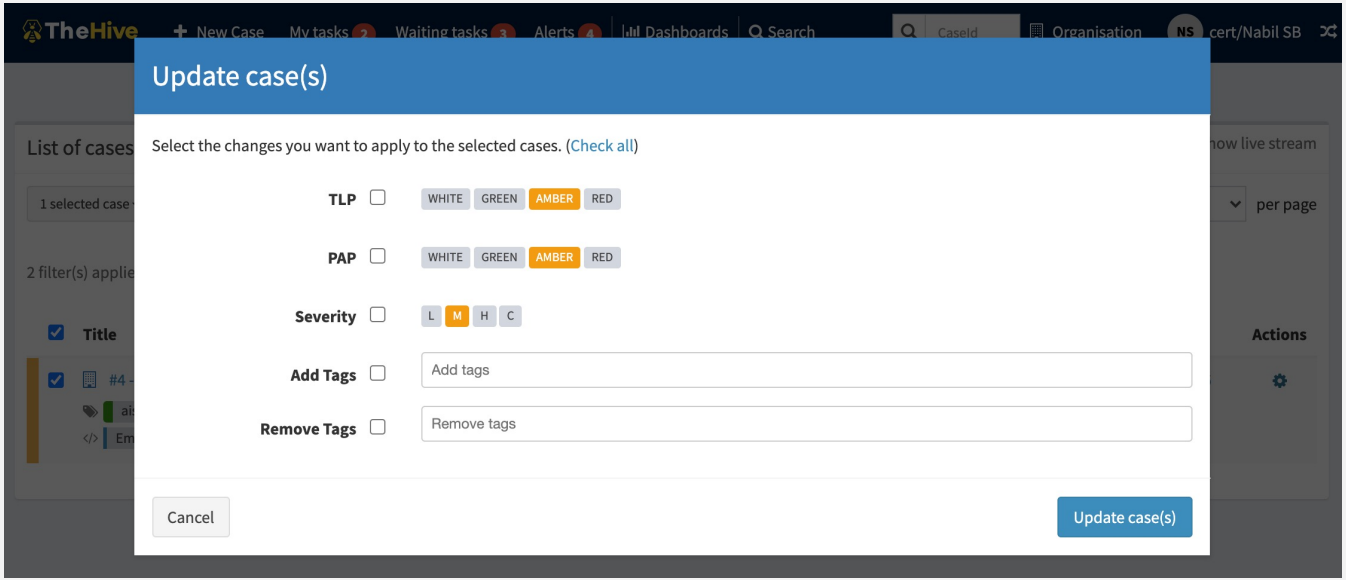
UI Improvements

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



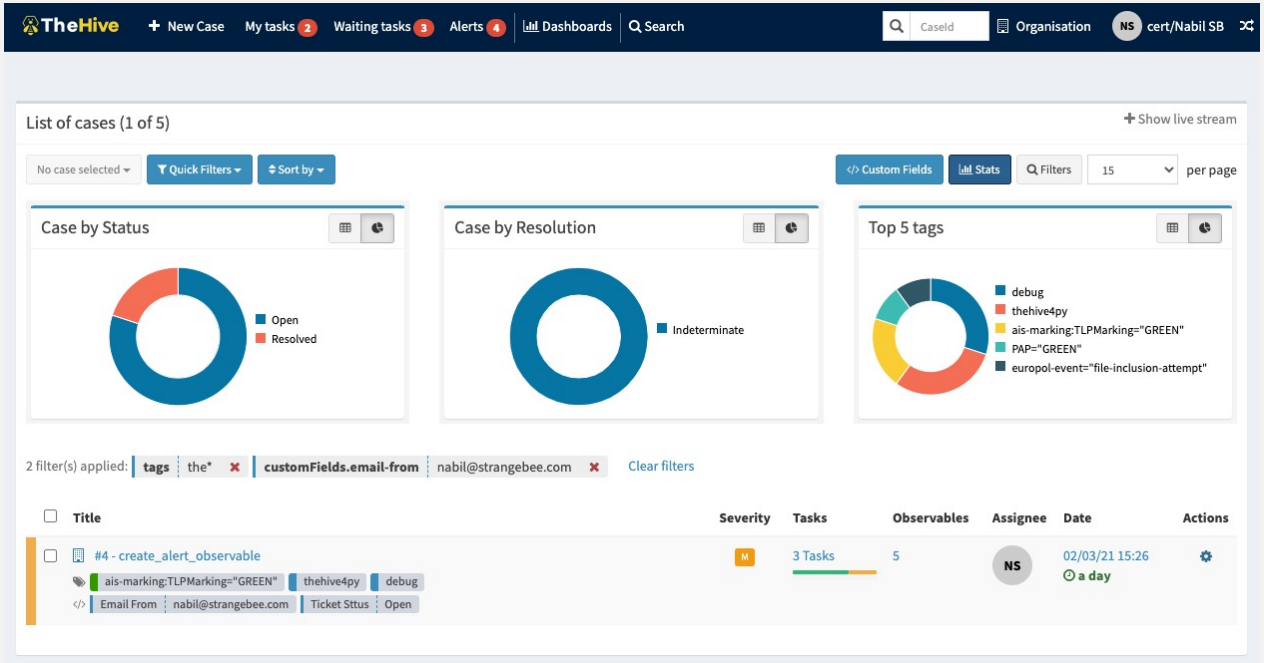
UI Improvements

- Bulk operations in case and observable lists



UI Improvements

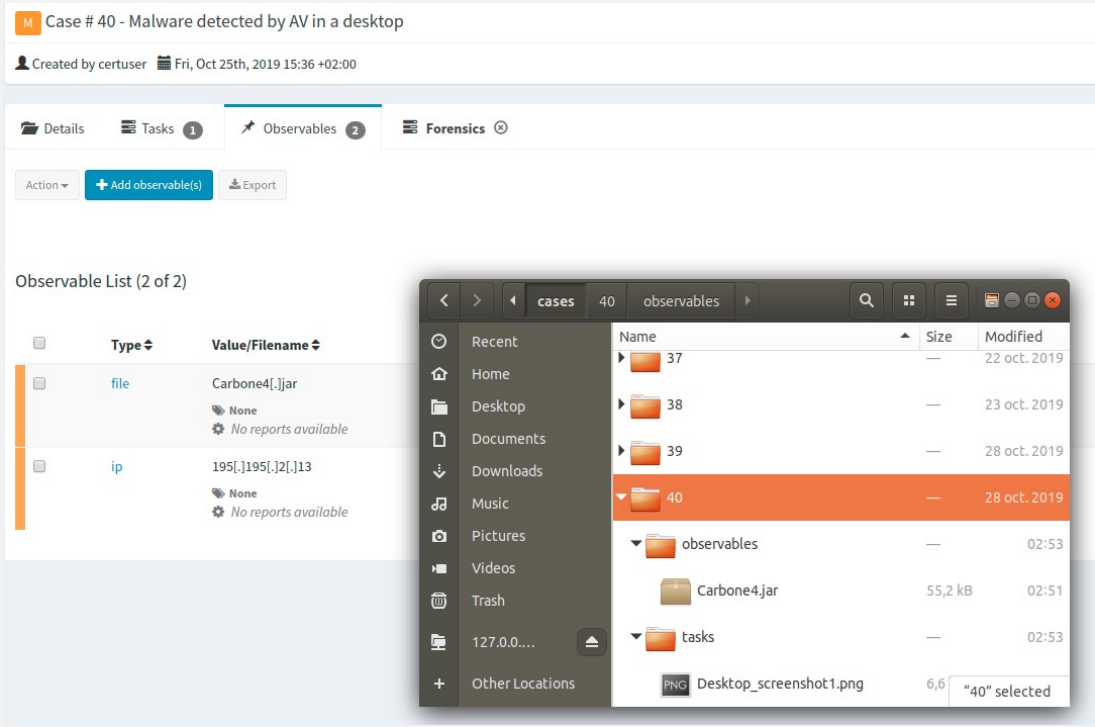
- Visual statistics in case, alert, observable lists



TheHive FS

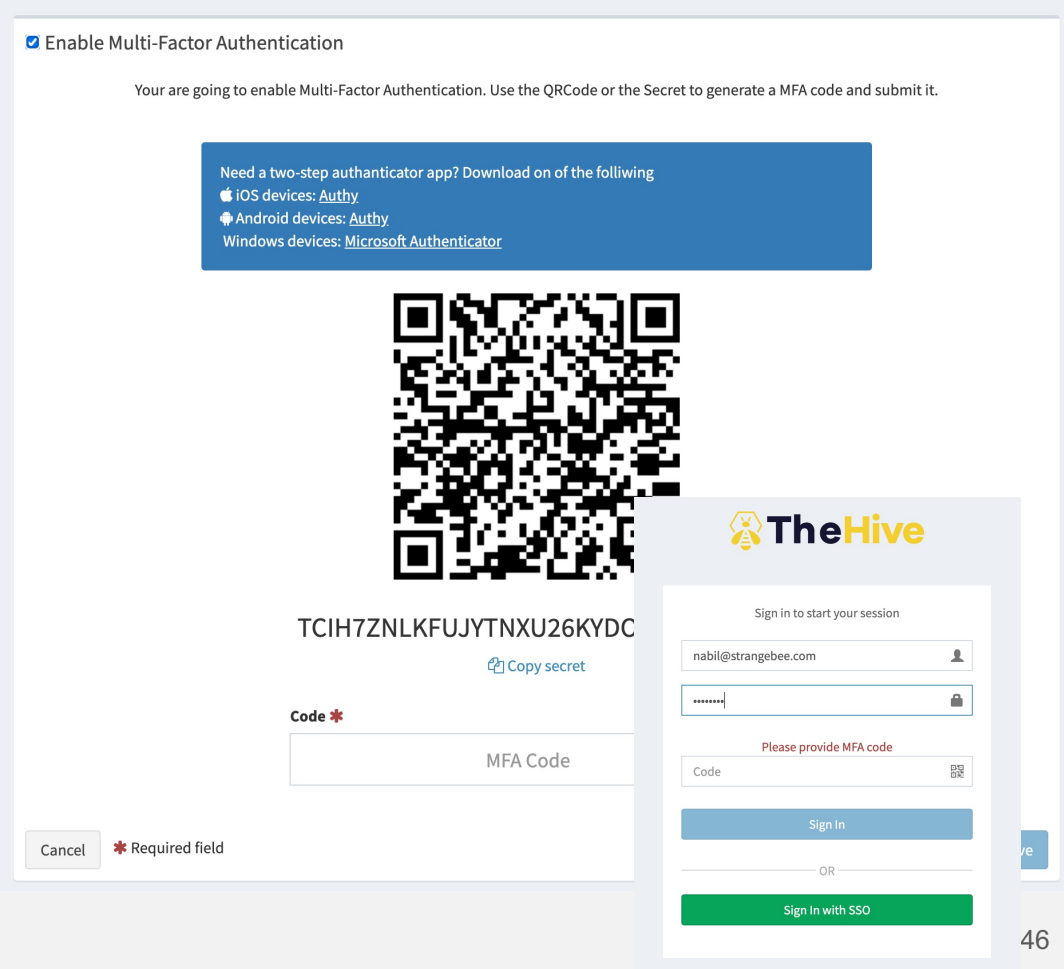
- Get quick access to files stored in TheHive directly from your investigation machine
- Connect remote webdav FS of TheHive

  `dav(s)://thehive:9001/fs`
- Use credentials of TheHive user
- Speed up investigation & analysis (but try not to step on a landmine)



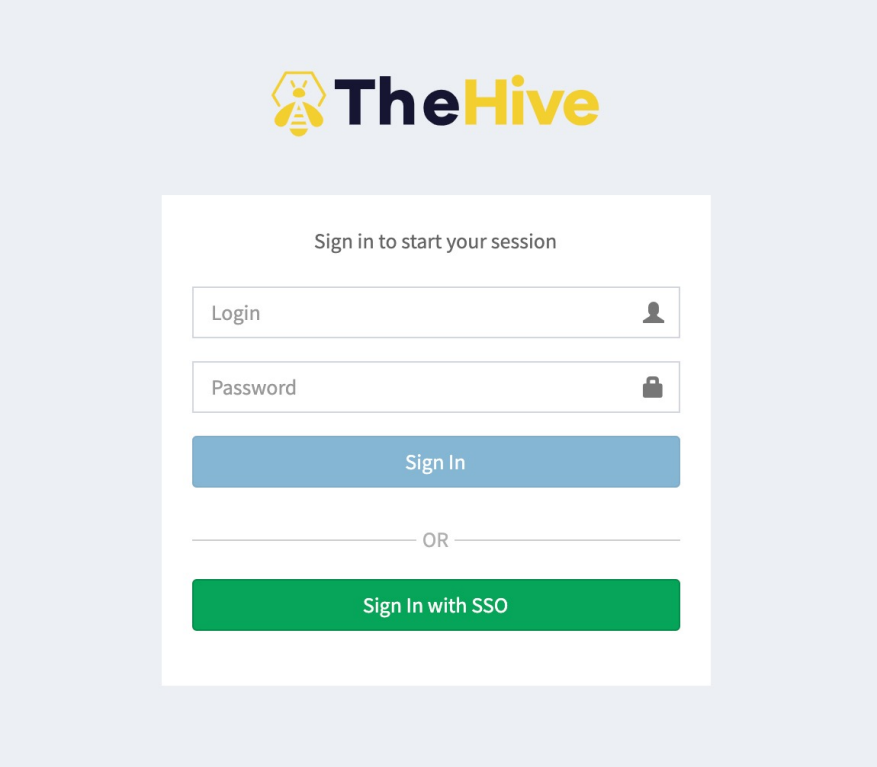
2FA Authentication

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



Single Sign On

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



StrangeBee

Need Help?

Thank You, any questions?

Community

https://blog.thehive-project.org

https://chat.thehive-project.org

https://twitter.com/TheHive_Project

users@thehive-project.org

https://www.strangebee.com

contact@strangebee.com

StrangeBee