Filigran

Community Meetup

December 2024 - Lyon

Our Team

Jean-Philippe Salles

VP of Product Management

Constant Bridon

VP of Data Engineering

Nicolas Quintin

Lead CSM

Jean-Baptiste Orozco

Product Owner - OpenBAS

Margaux Chatelet

Marketing Manager

Agenda

1. | ROADMAP
2. | DATA ENGINEERING
3. | OPENCTI DEMO
4. | OPENBAS DEMO
5. | COMMUNITY STORY

1. ROADMAP

What to expect in the coming months?

OpenCTI Strategic Roadmap

Common Deliverables

- NLP Text-to-stix auto extraction EE
- Ingesting Yara file, emails
- Disseminating deliverables EE

Ingestion performance

- Data preparation for deconfliction
- Reduce congestion in queue
- Manual workflow improvement

PIRs & Profile

- PIR to drive platform configuration EE
- Custom views
- Auto-alerting based on PIRs EE

Reducing MTTD/MTTR

- Better Case management workflow
- Correlation engine EE
- Graph & timeline improvement

Gaps analysis

- Alerts on intel gaps EE
- Qualifying Intel sources EE
- Scoring analysis

Adversarial Exposure

- Simulating threat from OpenCTI
- Comparing ATT&CK coverage
- Highlight of top threat priorities EE

OpenBAS Strategic Roadmap

Continuous testing

- Continuous Atomic testing
- Detection rule speed and efficiency
- Control Point surveillance EE

Realistic simulation

- Phishing campaign
- Conditional execution of events
- Stakeholders Persona simulation EE

Actionable Assessment

- Assessment deliverables
- Customizable Security Posture Dashboard EE
- Tailored recommendations EE

Leveraging CTI

- IoCs from OpenCTI
- Automating Assessment from OpenCTI EE
- Threat exposure adaptation from OpenCTI

Human skills assessment

- Skills and Skillsets
- Players' skill efficiency as Control point
- Import of cybersecurity Skills framework

Live simulation interaction

- Increasing performances
- Players <-> Animation team interaction
- Interactive timeline

XTM Hub Strategic Roadmap

Vision

Sharing is mandatory for the cybersecurity community. **XTM Hub is a central forum**, where members of the Filigran community (free users, customers, integrators, partners) **find resources & tradecrafts to improve usage of Filigran's products**.

Community growth

- Partners documents vault
- Highlight of Ambassadors & Users

Onboarding & sharing

- One-click deployment of Dashboards, …
- Trial version
- Self-service connector deployment

Users & Usage metrics

- Platform enrollment
- Identifying Organization's real engagement
- Feature usage in enrolled platforms

2. DATA ENGINEERING

Why? How? What?

A brief history of time

September 2022

Filigran's founding,
out of Samuel &
Julien's brilliant minds

June 2023

Seed round
5M €

March 2024

A - Series
15M €

October 2024

B - Series
35M $

A brief history of time

September 2022

Filigran's founding,
out of Samuel &
Julien's brilliant minds

June 2023

Seed round
5M €

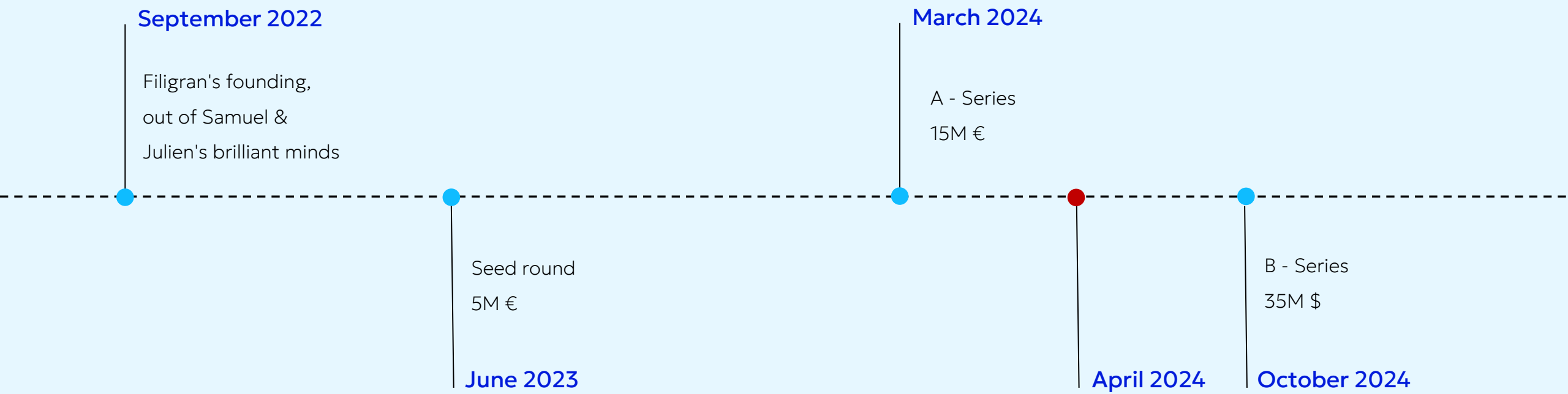
March 2024

A - Series
15M €

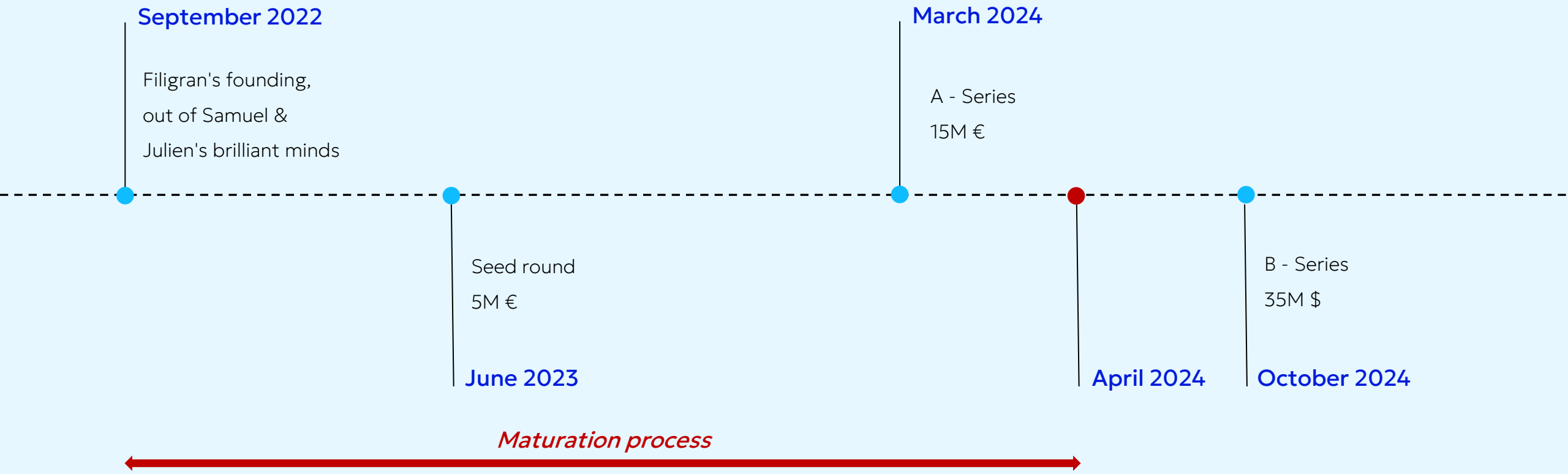
October 2024

B - Series
35M $

A brief history of time



A brief history of time



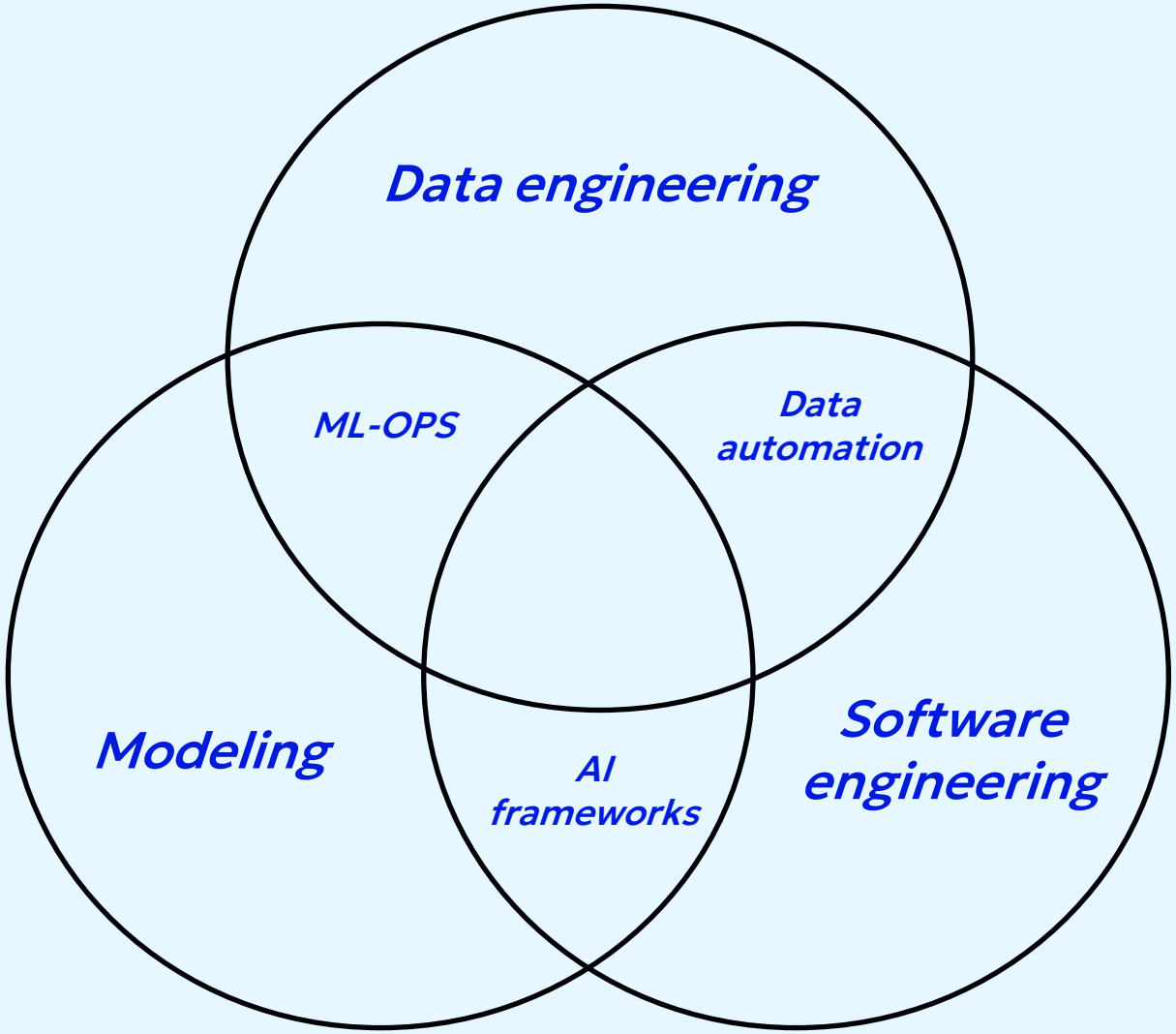
Why - AI ?

Sustain the growth of our products and company by leveraging data from our products and our company

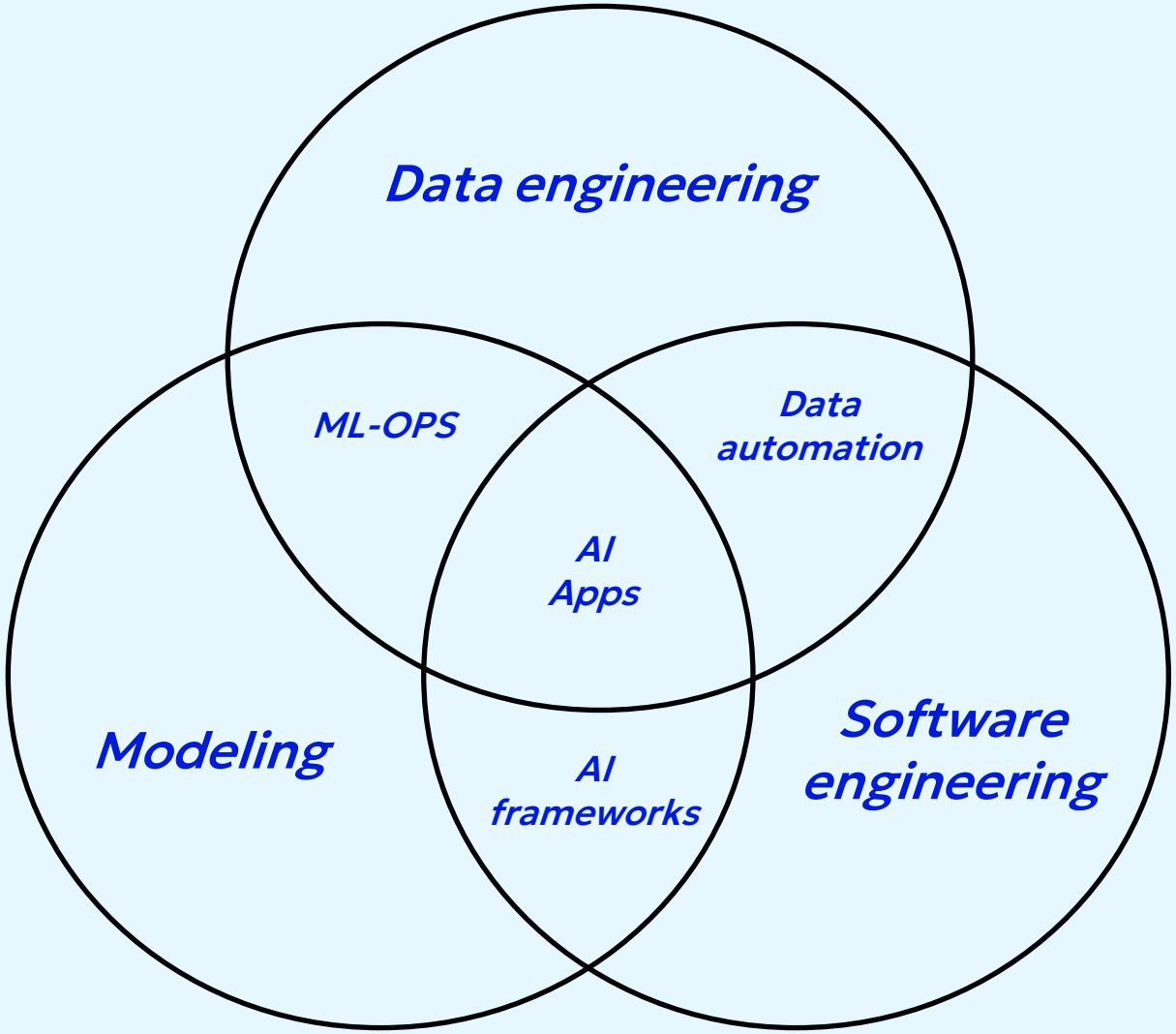
- Does not compete with Community Edition, but provides something additional that clients are ready to pay for

Usual data landscape

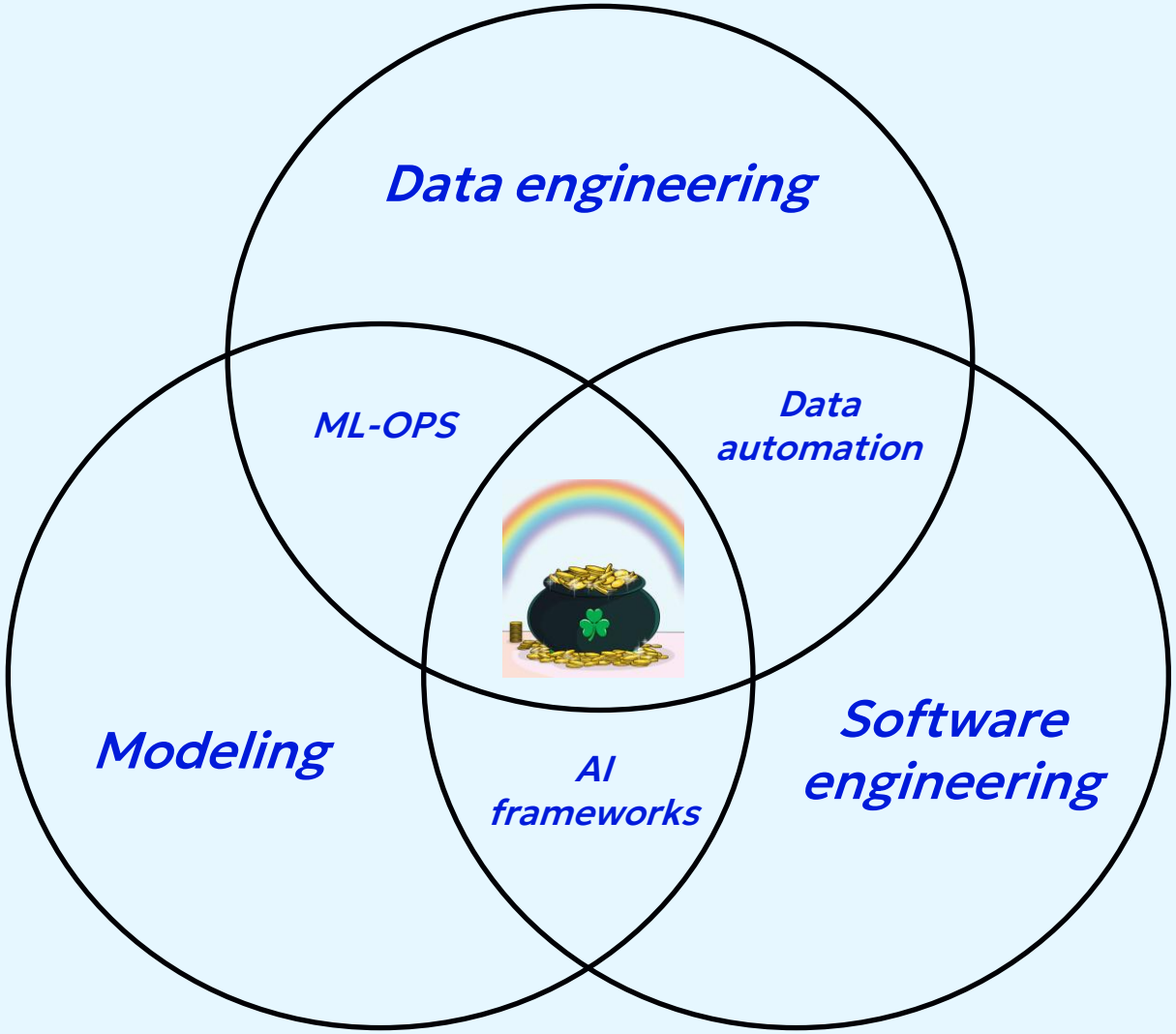
Usual data landscape



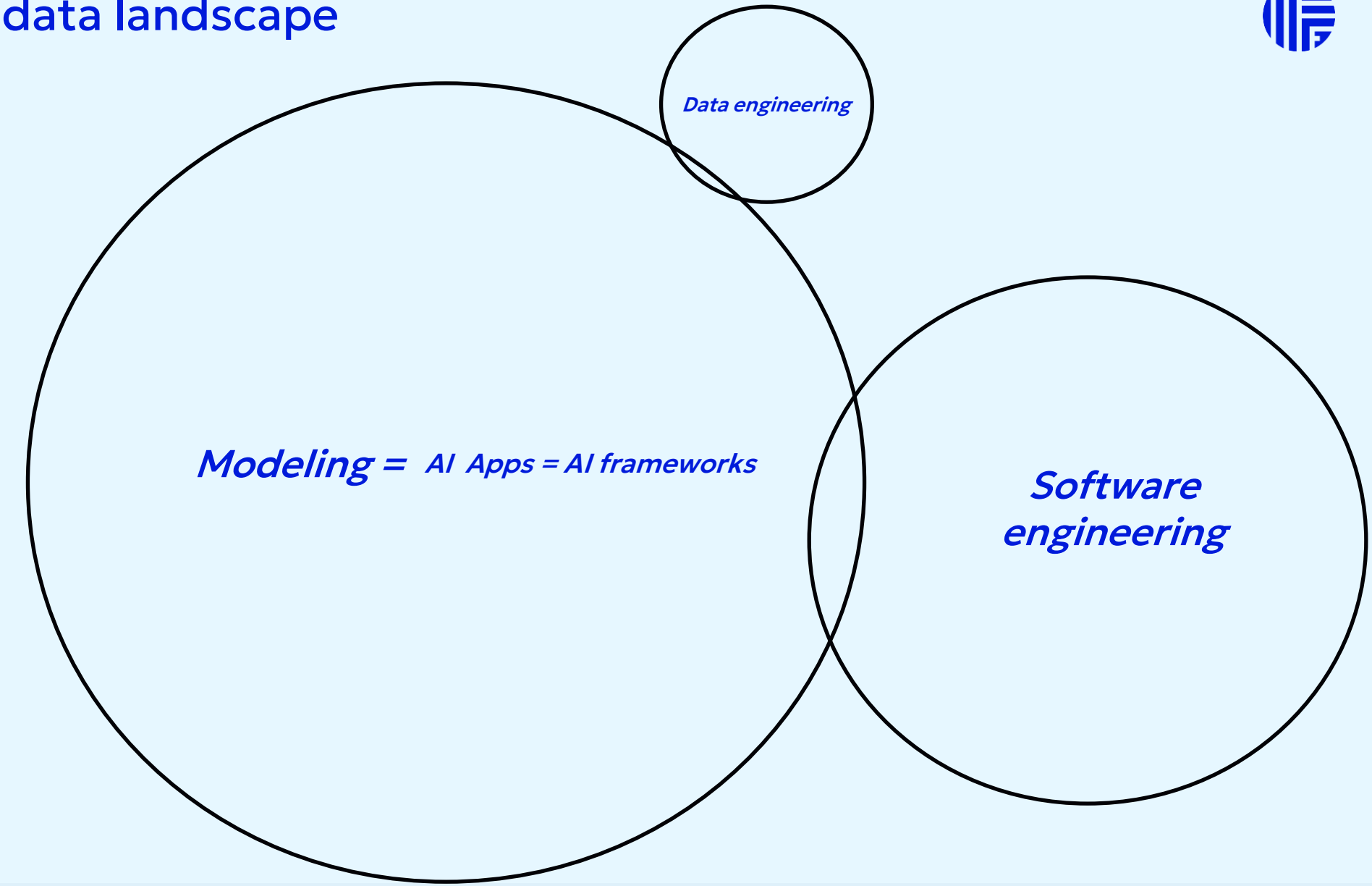
Usual data landscape



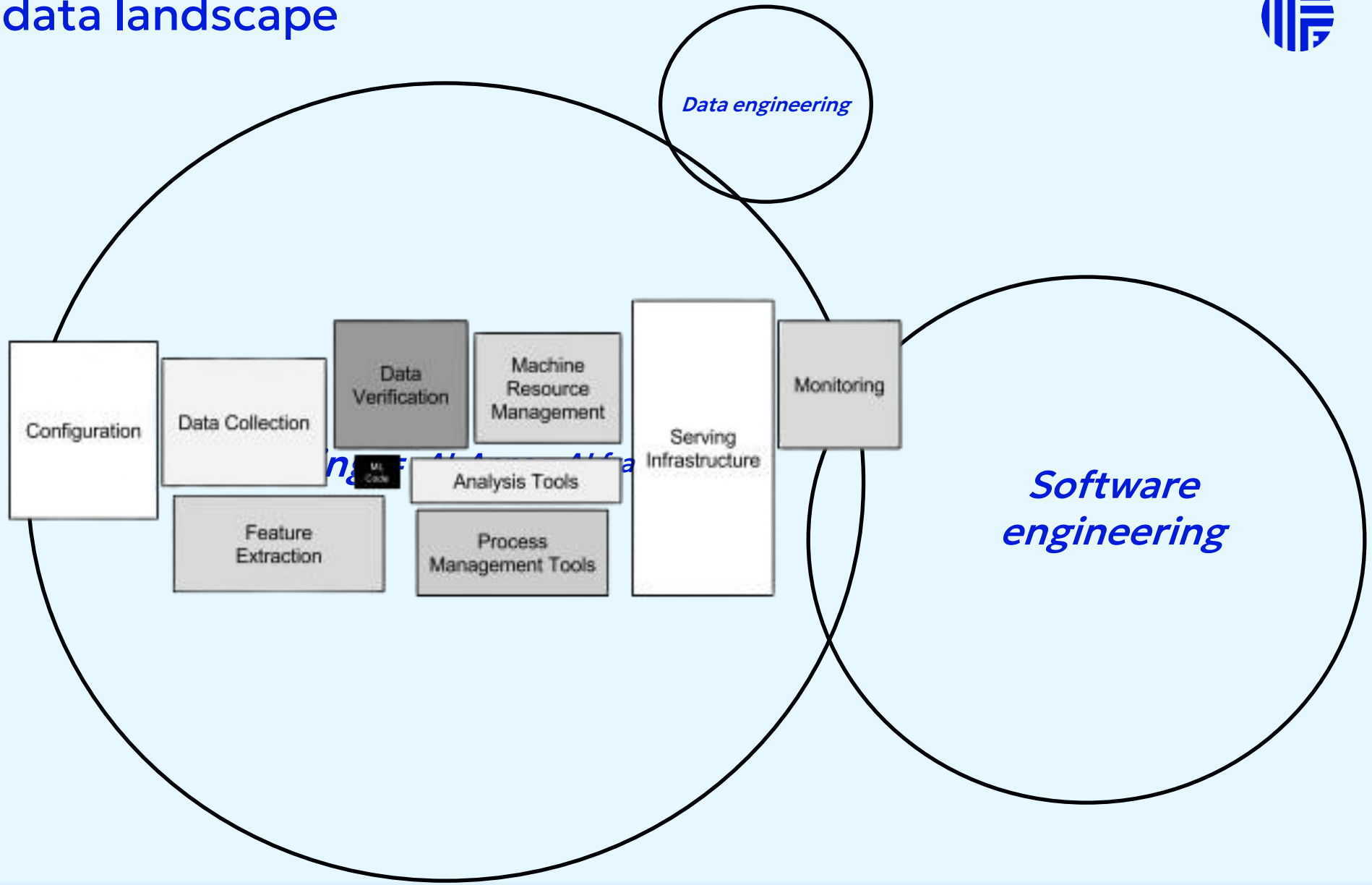
Usual data landscape



Percieved data landscape

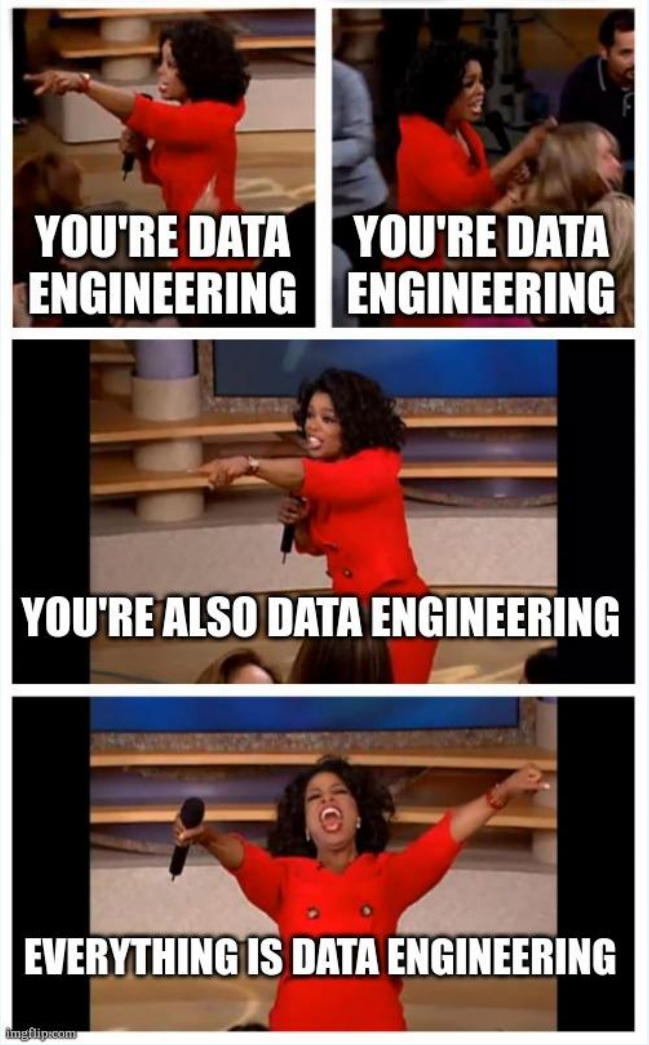


Percieved data landscape

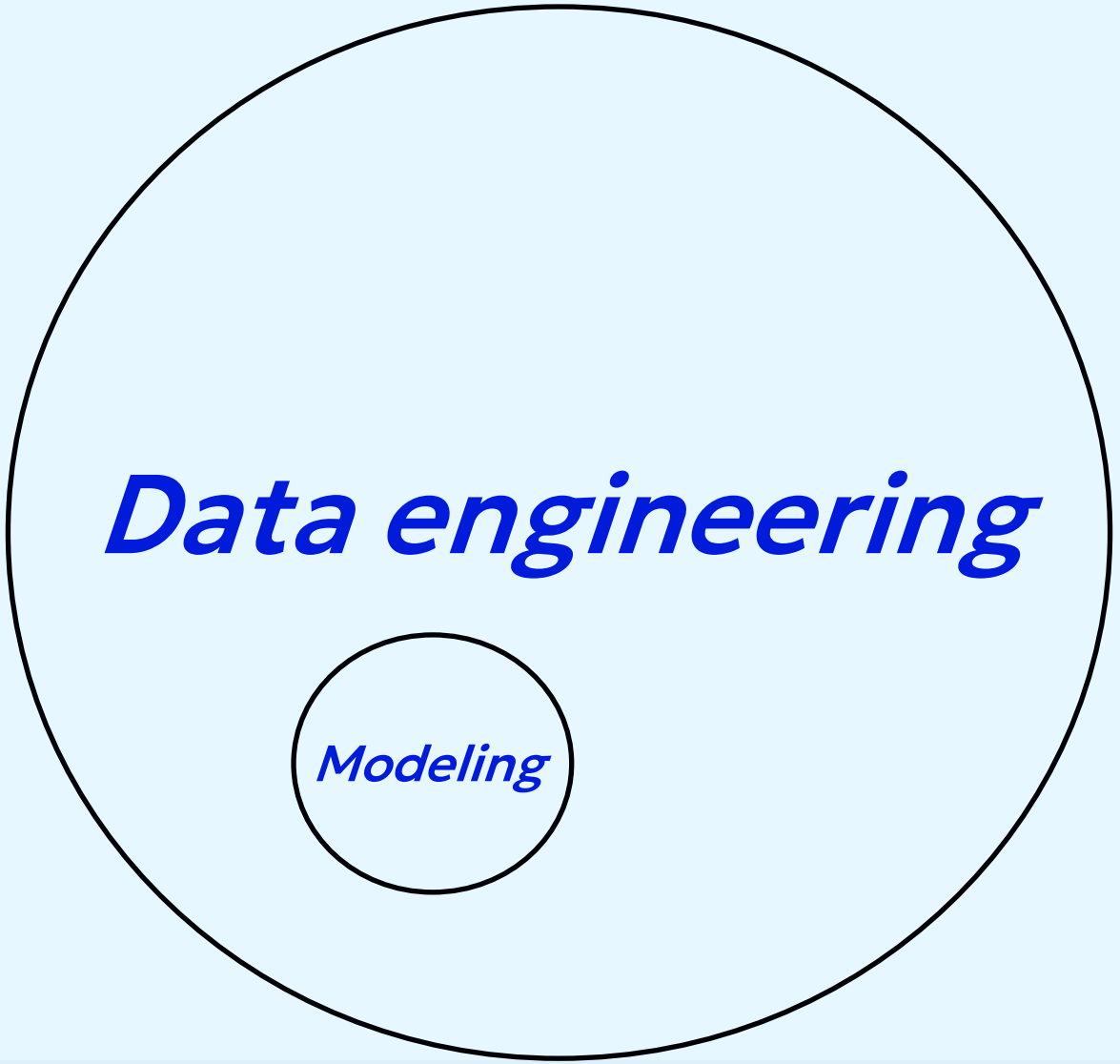


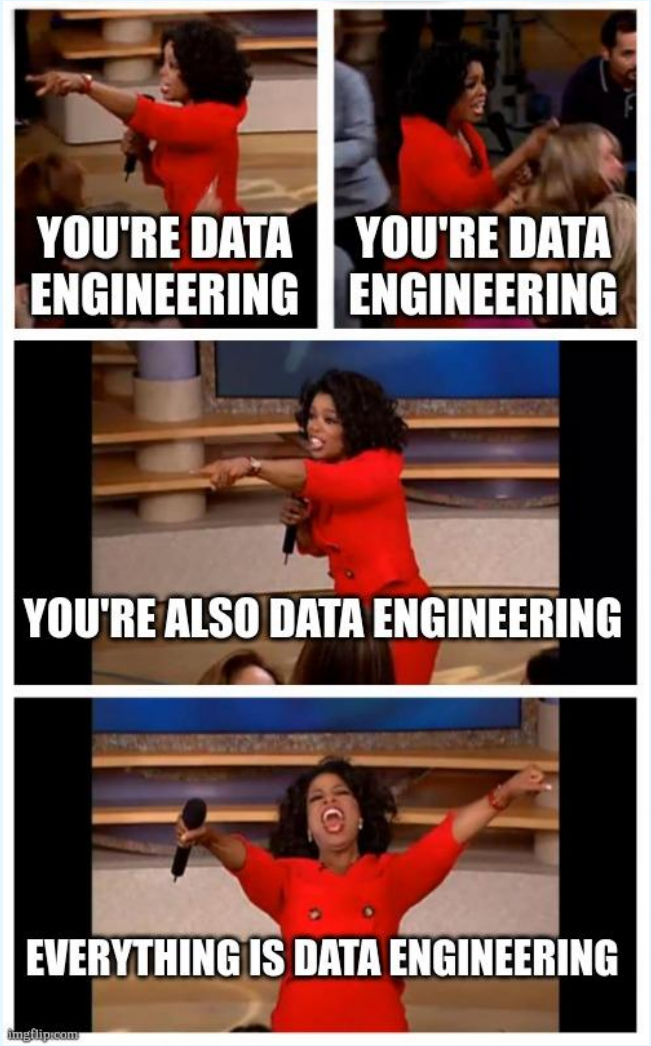
How - Our data landscape

Data engineering



How - Our data landscape





What - Use cases

OpenCTI

Extraction of Entities from Text

Automatic correlation when an object is added to the platform

OpenBAS

Generation of relevant payloads

Cross product

Generate OBAS scenari from OCTI infos

What - Use cases

OpenCTI

Extraction of Entities from Text

Automatic correlation when an object is added to the platform

OpenBAS

Generation of relevant payloads

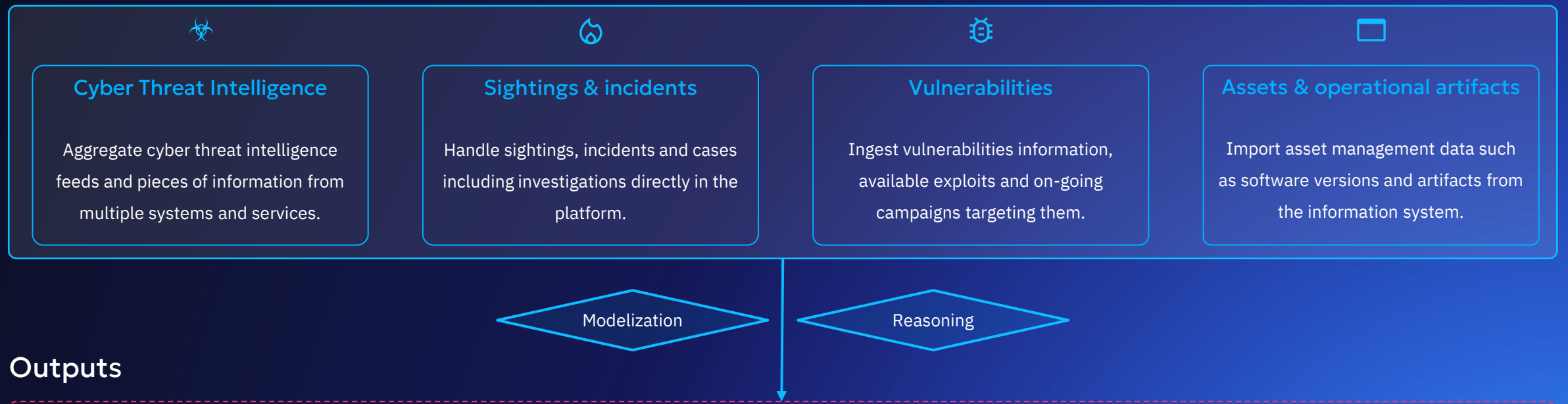
Cross product

Generate OBAS scenari from OCTI infos

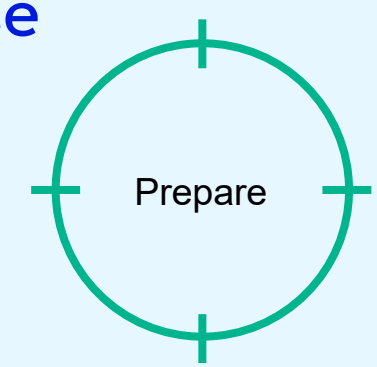
3. OPENCTI

Overview and Demo

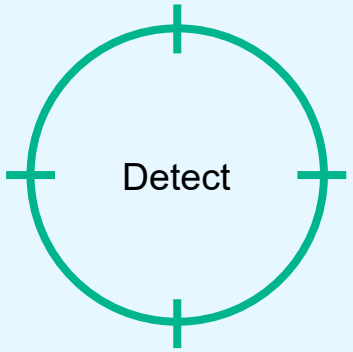
OpenCTI Overview



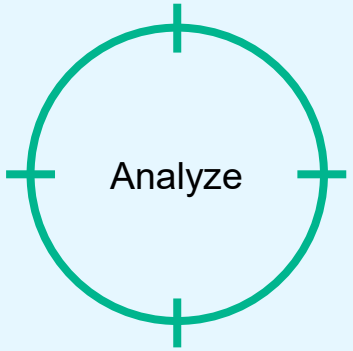
Workflow: Incident Response



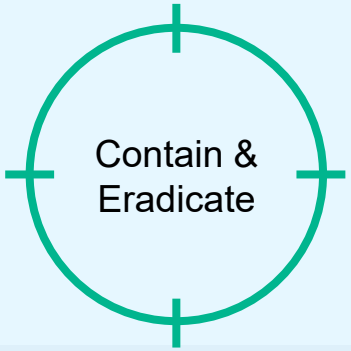
In OpenCTI :
Create **workflow status**, **vocabularies**, **task templates** and **labels** for each relevant entity (incidents, events, narratives, channels, individuals, etc.).
Create **RFI, RFT and Incident Response Cases workflows** with task templates assigned to operators.



Plug **connectors** to immediately ingest information on Incidents.
Create **playbooks** to automatically create incidents with an assignee as soon as content is detected, to reduce MTD.

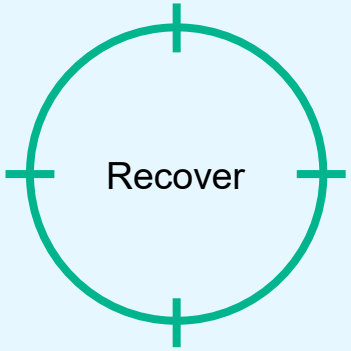


If the incident created is relevant, trigger a **playbook** that will add it to an **incident response case**, add **tasks** and **enrich information** based on your CTI.
By following the tasks, **analysts add** all relevant **entities and relations** to the case.
Analysts **start writing** in the **content** area of the case.



At the case level, the **analysts add RFI** to enrich the content and **RFT to disable attacker infra**.
Each **container is assigned to the right person,** so you act collectively with the overall content of the case.

Once the incident has been contained, the **status** of the case **changes to "completed"**.
The case is archived for replay in OpenBAS to identify areas for improvement and the teams' defense posture.



With the help of **RFI**, the decision-maker guides the production of content to guide the recovering process. He can use **notes**.
He **can export** investigative content and counter-measures **in .pdf** format or share directly with the right teams.

4. OPENBAS

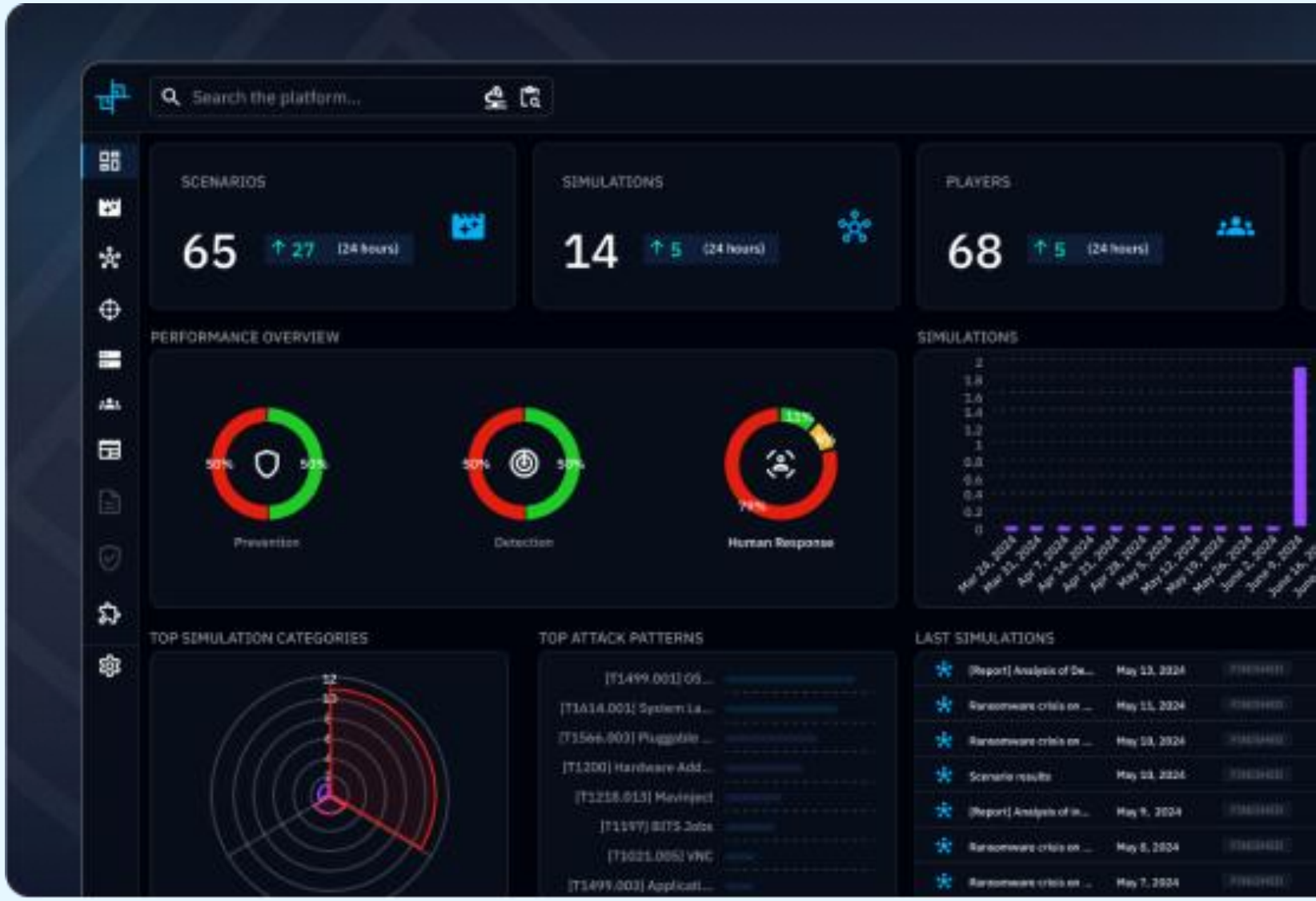
Overview and Demo

OpenBAS

OpenBAS is for cybersecurity managers who wants to :

- Evaluate Security Posture against Threats that matters
- Include all stakeholders in the evaluation
- Adapt their Security Posture to evolving Threat landscape and defensive capabilities

With **OpenBAS**, orchestrate your Security Posture evaluation through fully customizable Breach and Attack/Crisis Simulations, from technical payload injections to global media pressure.



Main use cases

Cyber attack simulation

Generate relevant Attack Scenario based on your qualified CTI data from OpenCTI.

Continuous testing

Have a Zero trust logic and follow up your security posture evolution by simulating complex scenario recurringly.

Security posture

Assess your Security posture through integration with your security platforms (SIEM, EDR, etc.).

Table-top exercise

Simulate non-technical aspects of a cyber attack, like emdia pressure, regulatory compliance, etc.

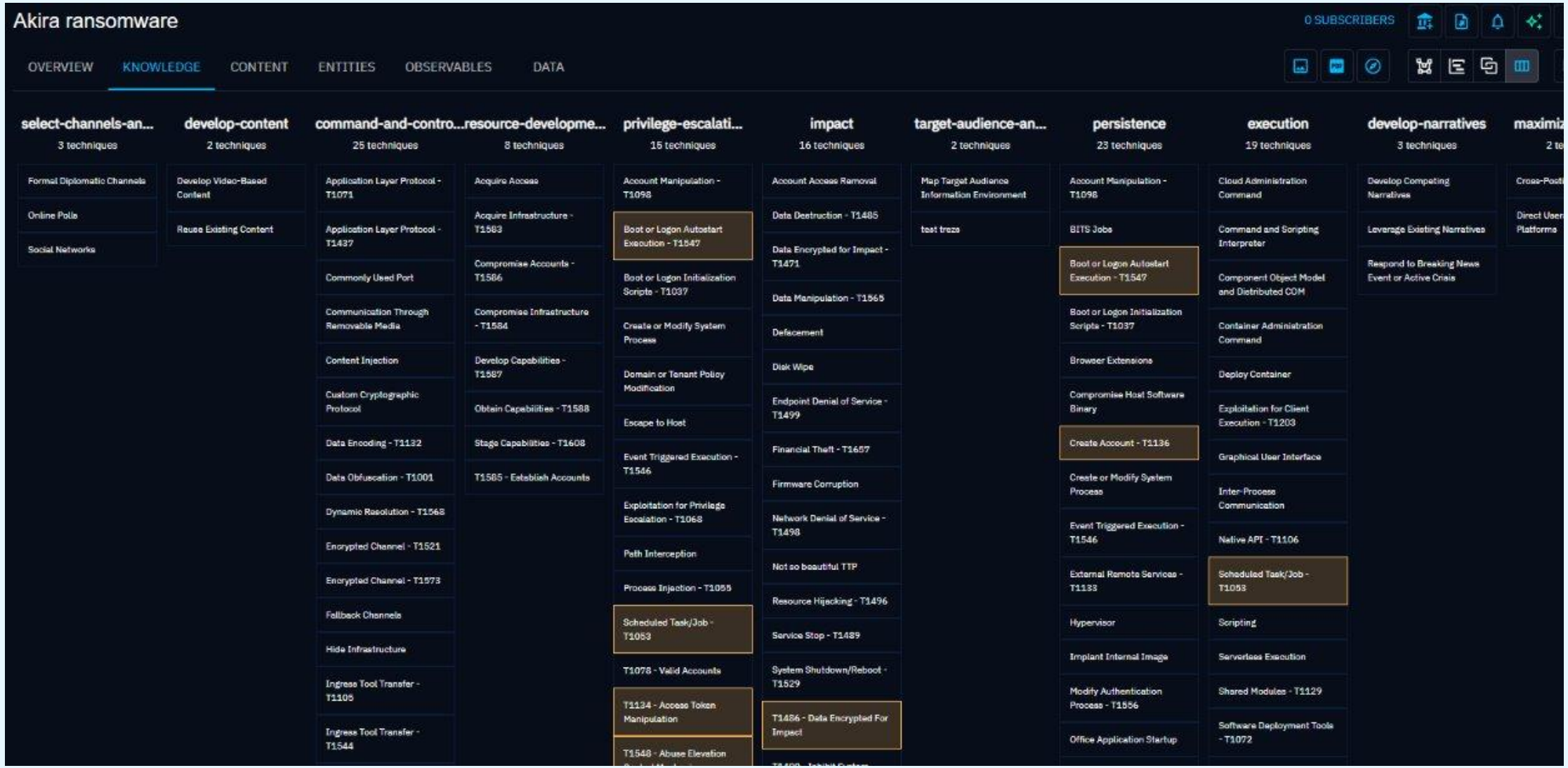
Atomic tests

Conduct atomic testing (technical and non-technical) to evaluate a Security Point.

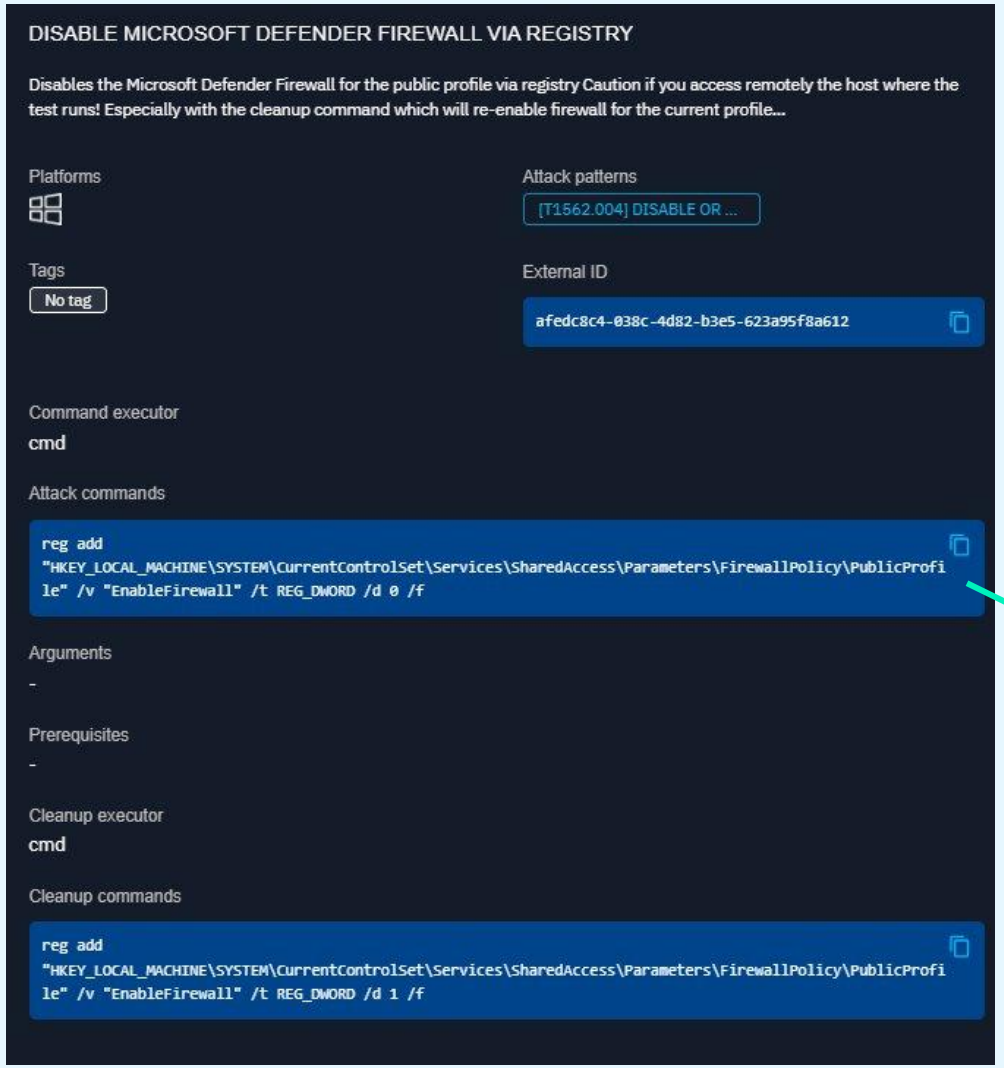
Reports generation

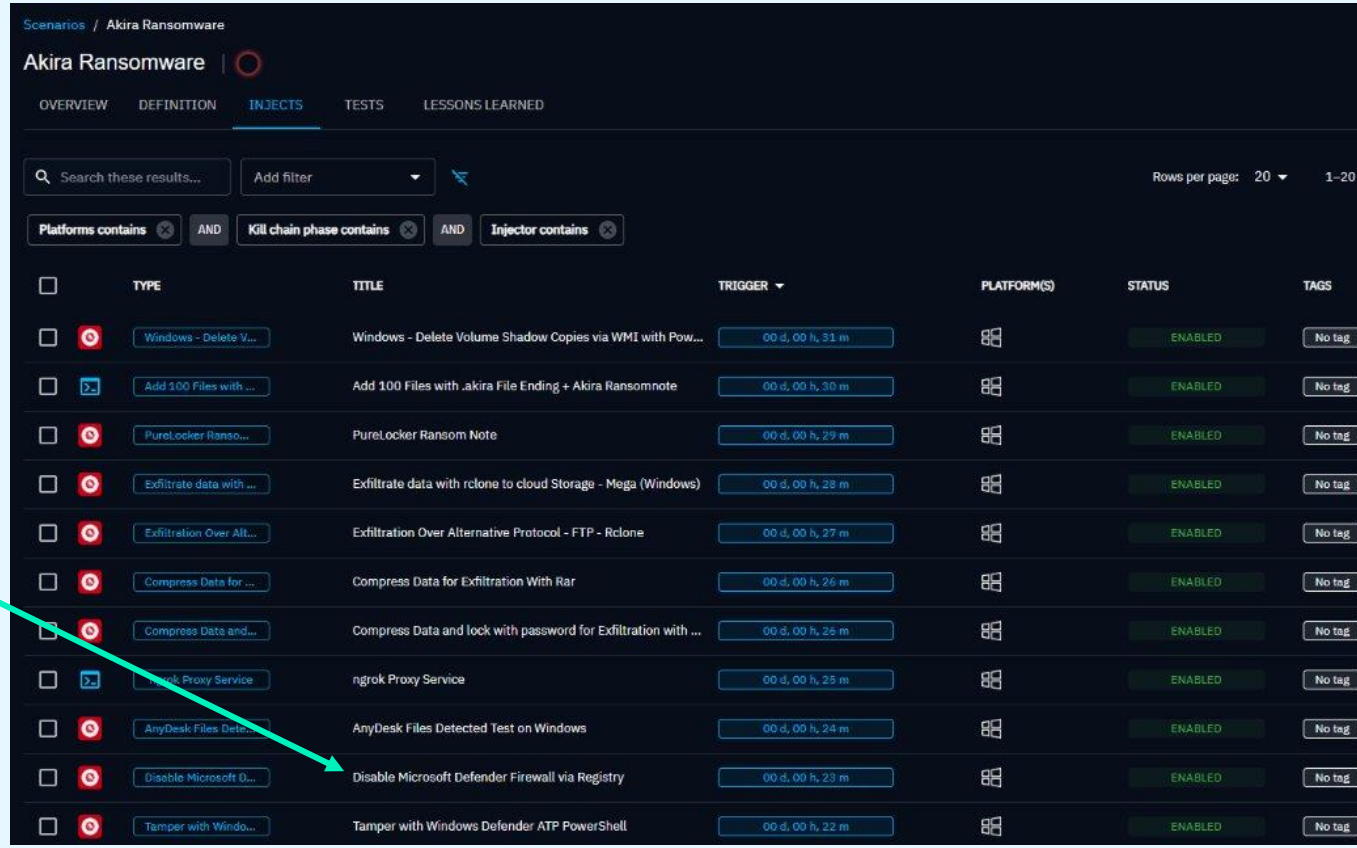
Based on the results of your simulation, generate and customize reports.

Use TTP to define attack patterns to mimic



Select payloads to inject on your assets





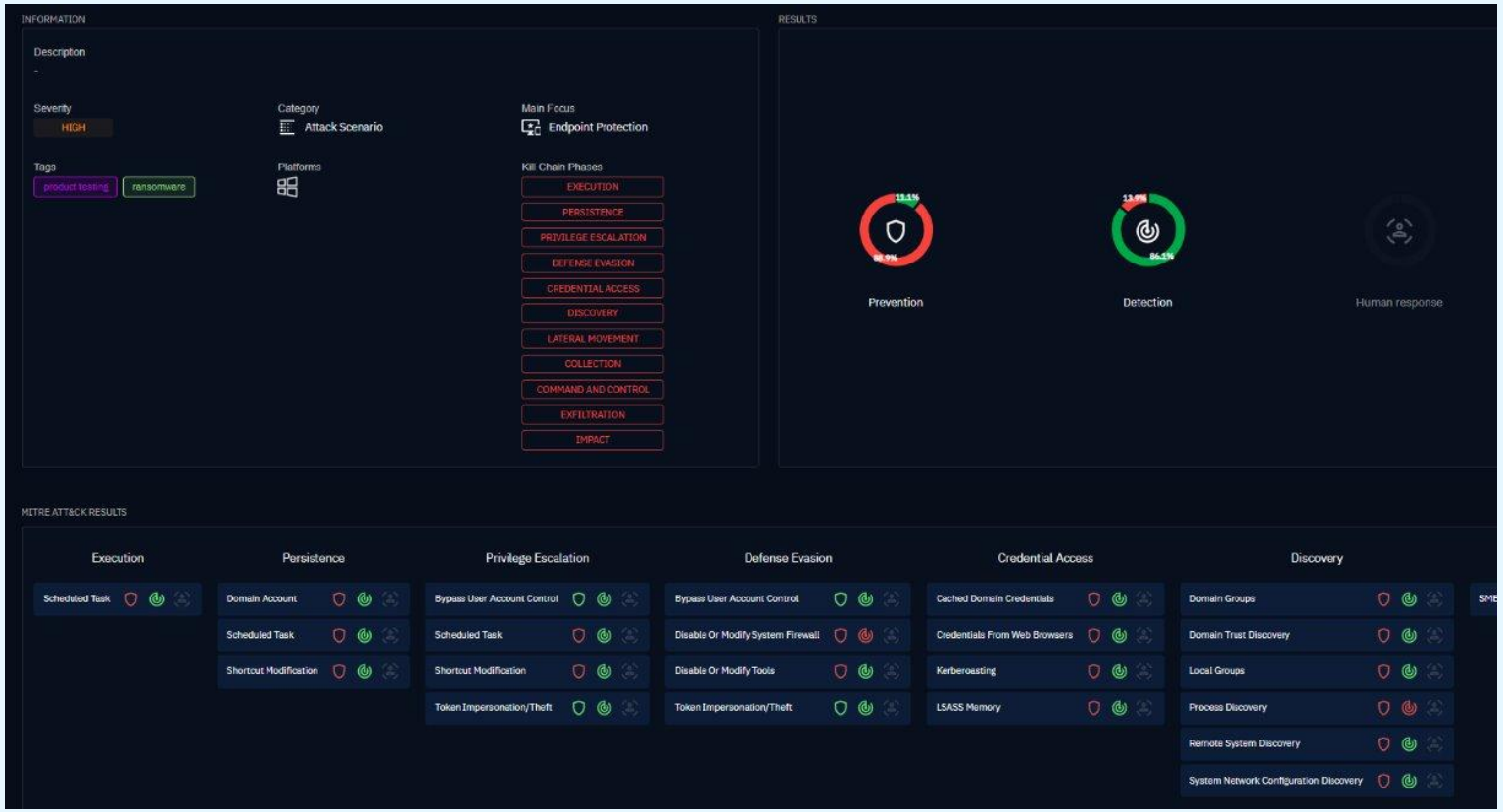
Get an overview of your security posture

Microsoft Defender

Microsoft Sentinel

CROWDSTRIKE

Coming soon



5. COMMUNITY STORY

Librairie GO

Thank you

Ask us anything

Filigran.io