



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?



Common Deliverables

NLP Text-to-stix auto extraction 

Ingesting Yara file, emails

Disseminating deliverables 

Ingestion performance

Data preparation for deconfliction

Reduce congestion in queue

Manual workflow improvement

PIRs & Profile

PIR to drive platform configuration 

Custom views

Auto-alerting based on PIRs 

Reducing MTTD/MTTR

Better Case management workflow

Correlation engine 

Graph & timeline improvement

Gaps analysis

Alerts on intel gaps 

Qualifying Intel sources 

Scoring analysis

Adversarial Exposure

Simulating threat from OpenCTI

Comparing ATT&CK coverage

Highlight of top threat priorities 



Continuous testing

Continuous Atomic testing

Detection rule speed and efficiency

Control Point surveillance 

Realistic simulation

Phishing campaign

Conditional execution of events

Stakeholders Persona simulation 

Actionable Assessment

Assessment deliverables

Customizable Security Posture Dashboard 

Tailored recommendations 

Leveraging CTI

IoCs from OpenCTI

Automating Assessment from OpenCTI 

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



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

Seed round
5M €

June 2023

March 2024

A - Series
15M €

B - Series
35M \$

October 2024

A brief history of time

September 2022

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

Seed round
5M €

June 2023

March 2024

A - Series
15M €

B - Series
35M \$

October 2024



A brief history of time



September 2022

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

Seed round
5M €

June 2023

March 2024

A - Series
15M €

April 2024

B - Series
35M \$

October 2024

A brief history of time



September 2022

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

Seed round
5M €

June 2023

March 2024

A - Series
15M €

April 2024

B - Series
35M \$

October 2024

Maturation process



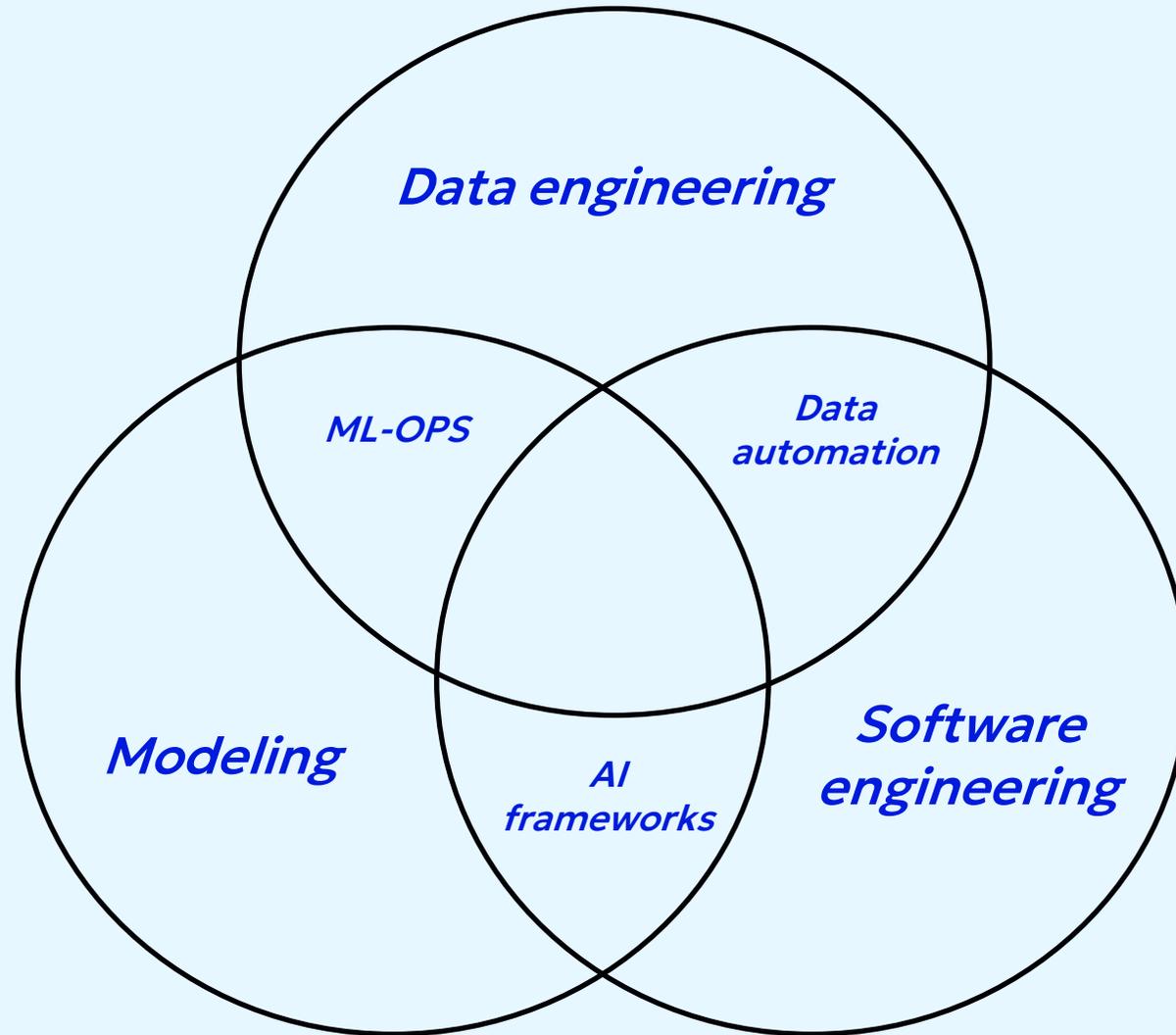
Sustain the growth of our products and company by leveraging data from our products and our company

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

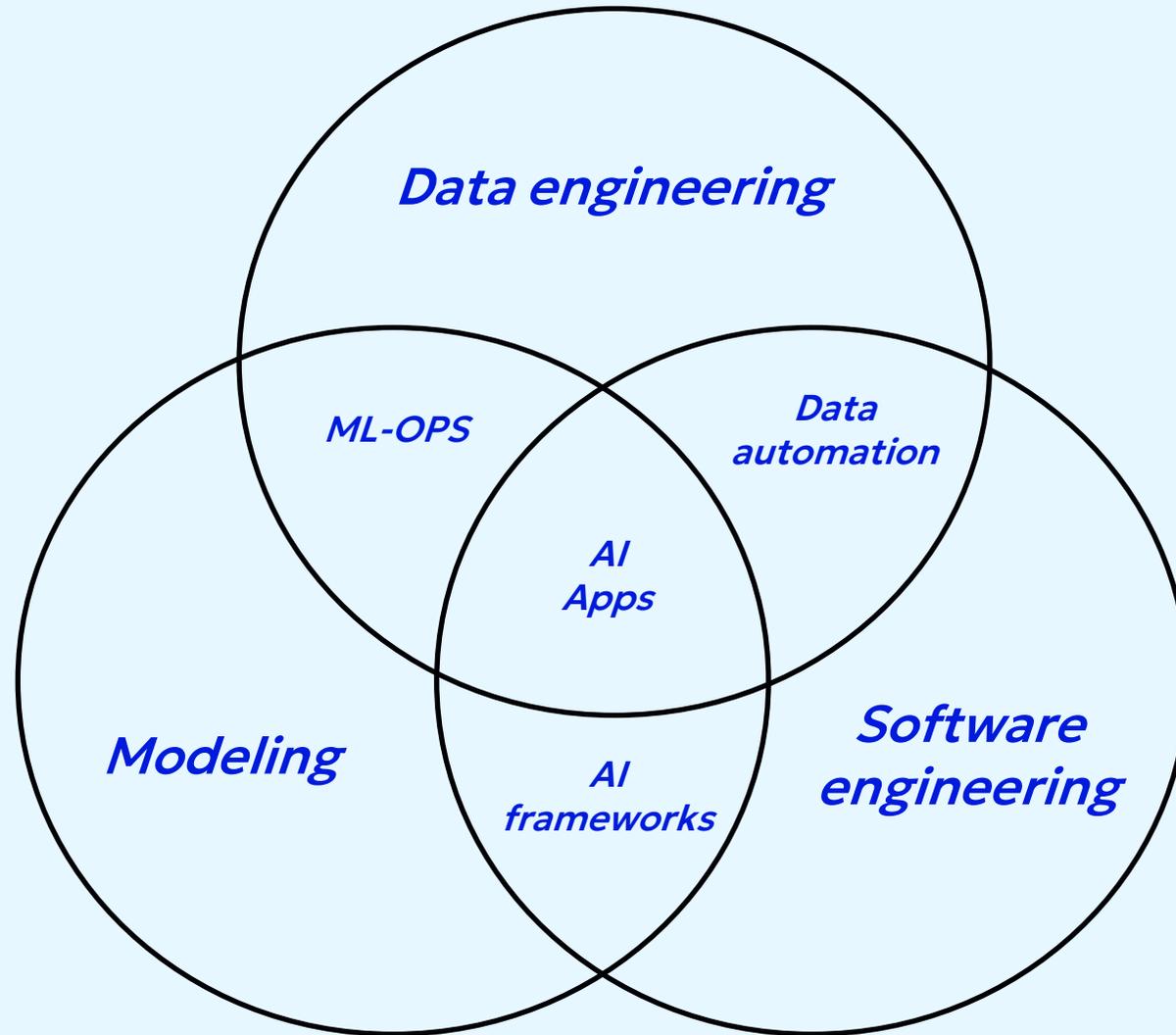
Usual data landscape



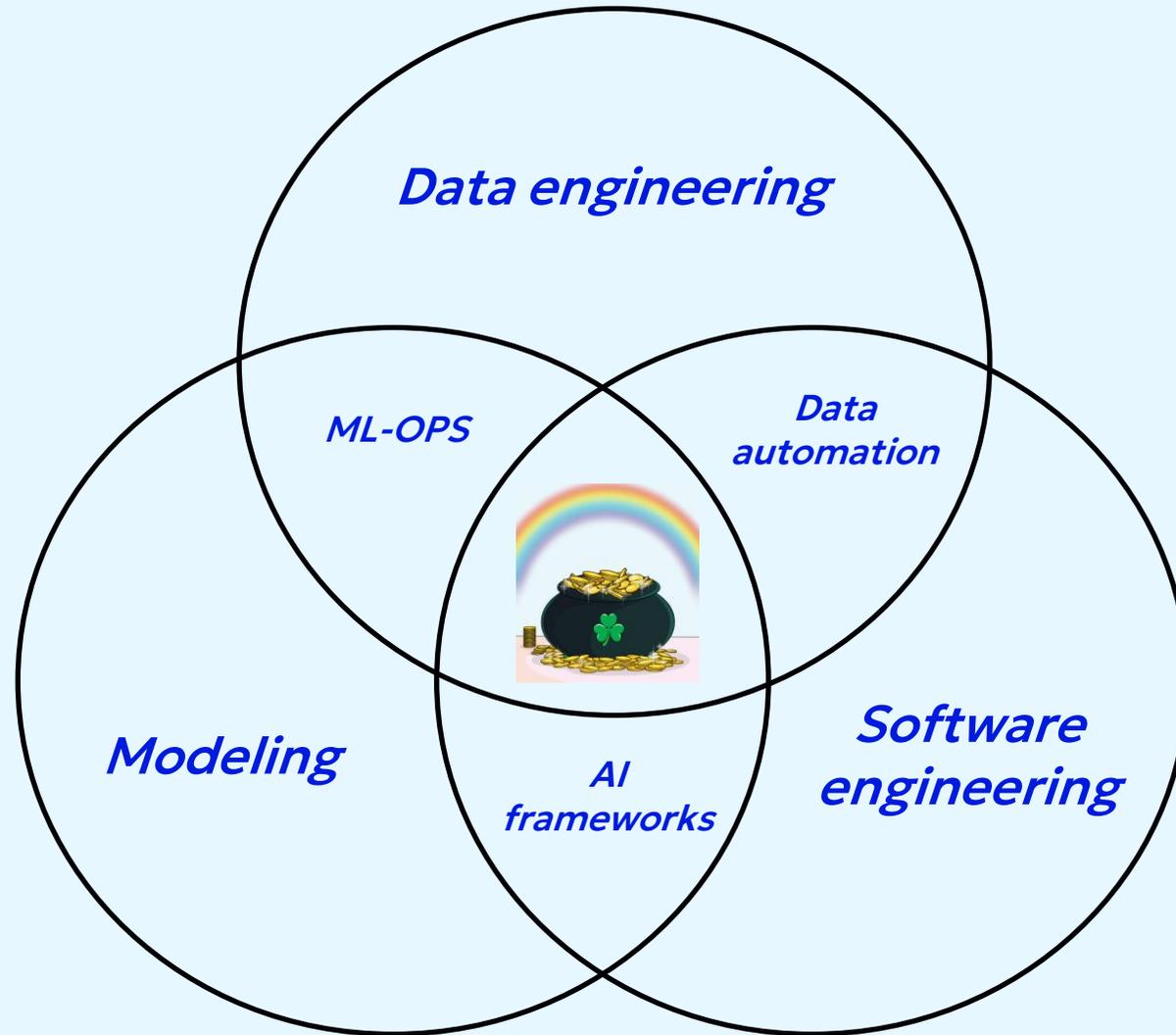
Usual data landscape



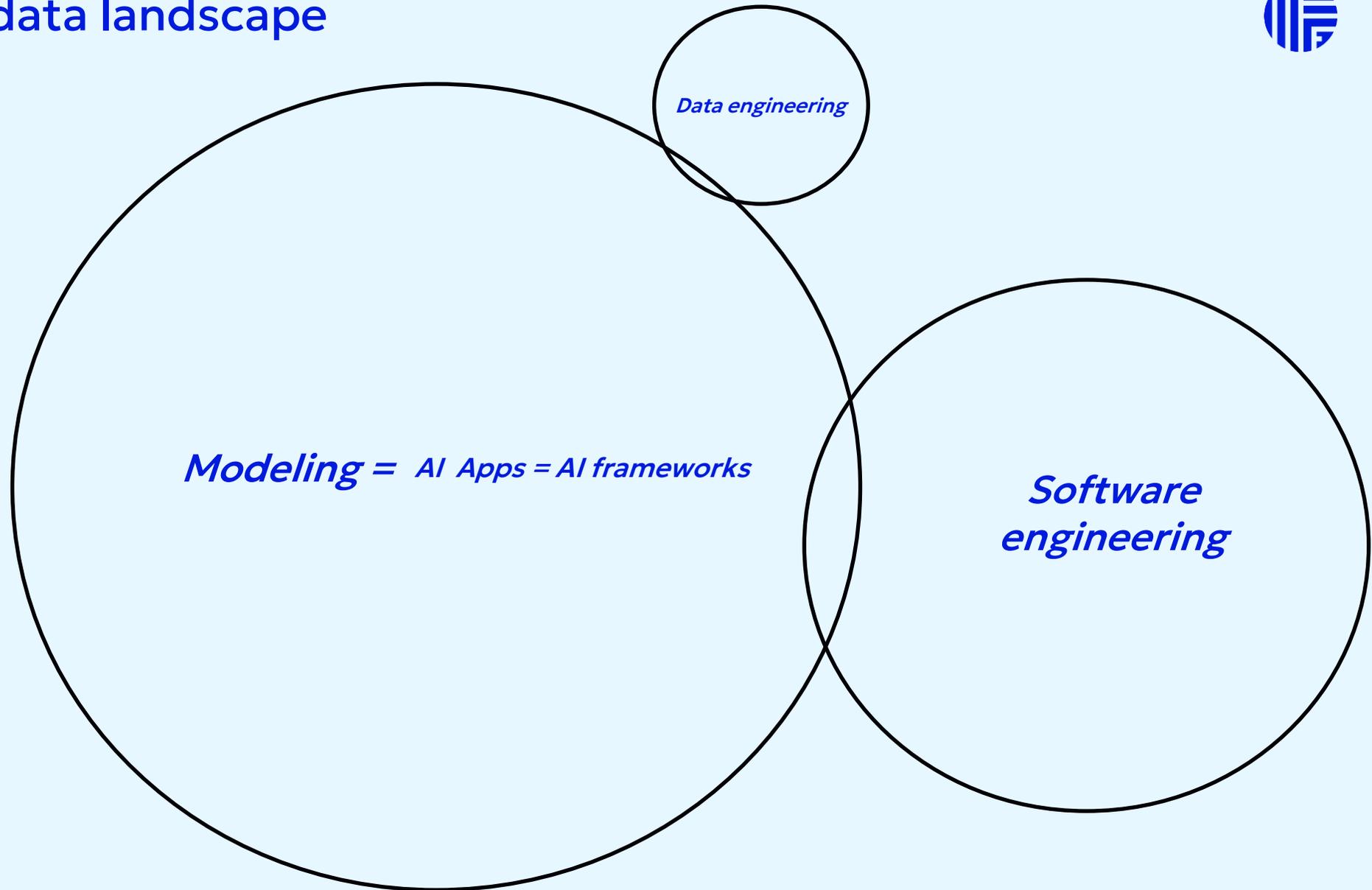
Usual data landscape



Usual data landscape

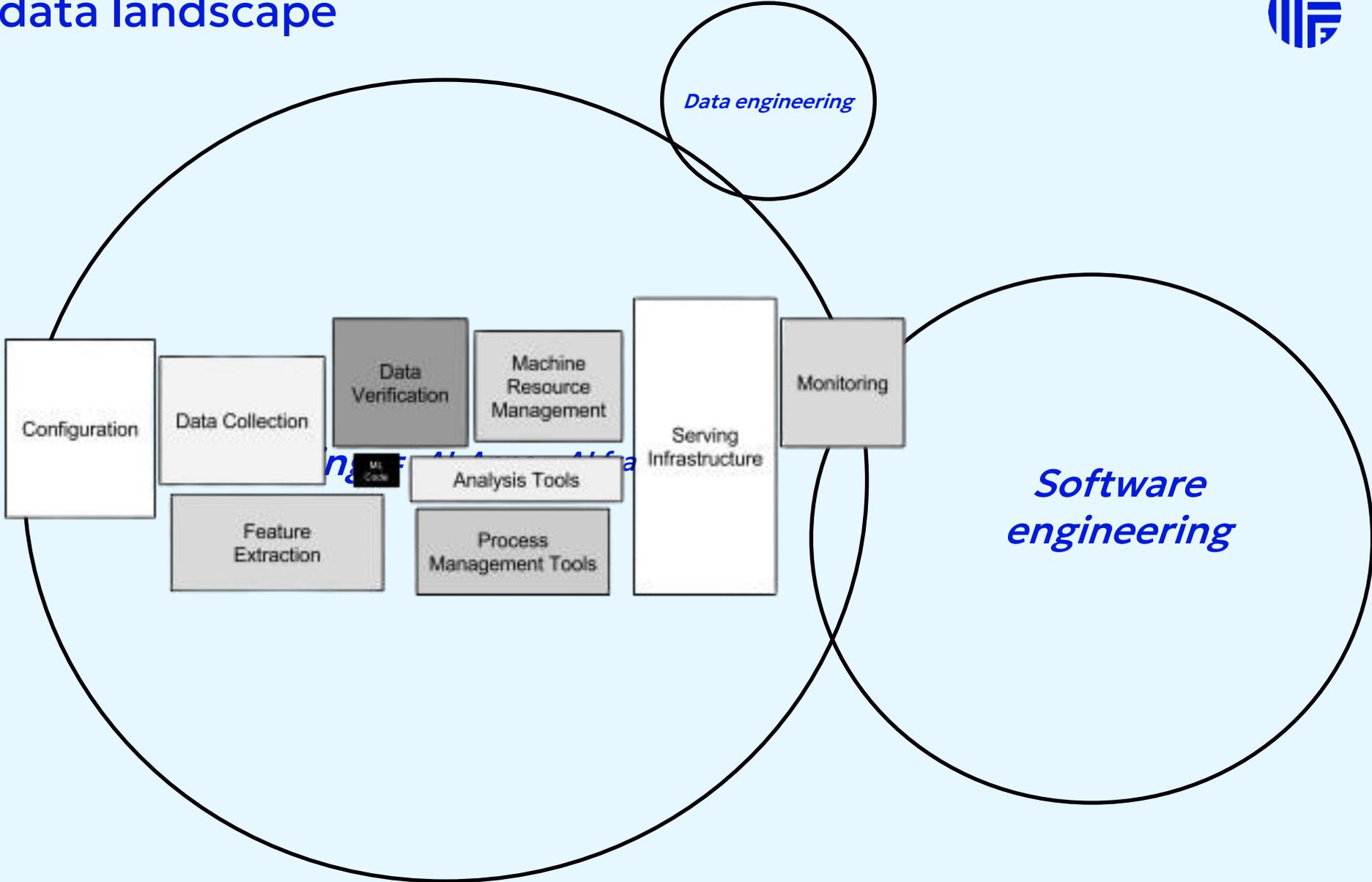


Percieved data landscape

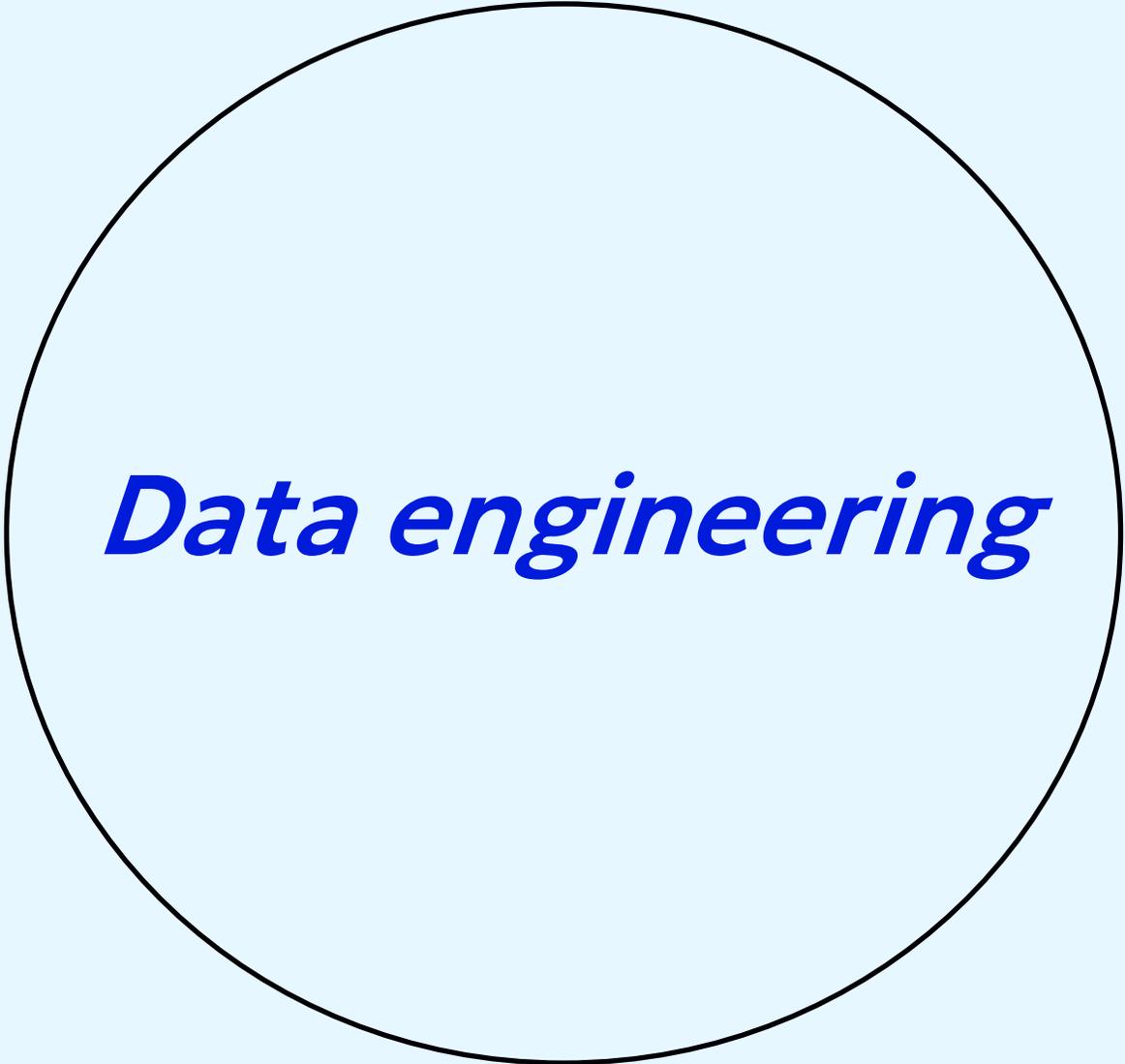




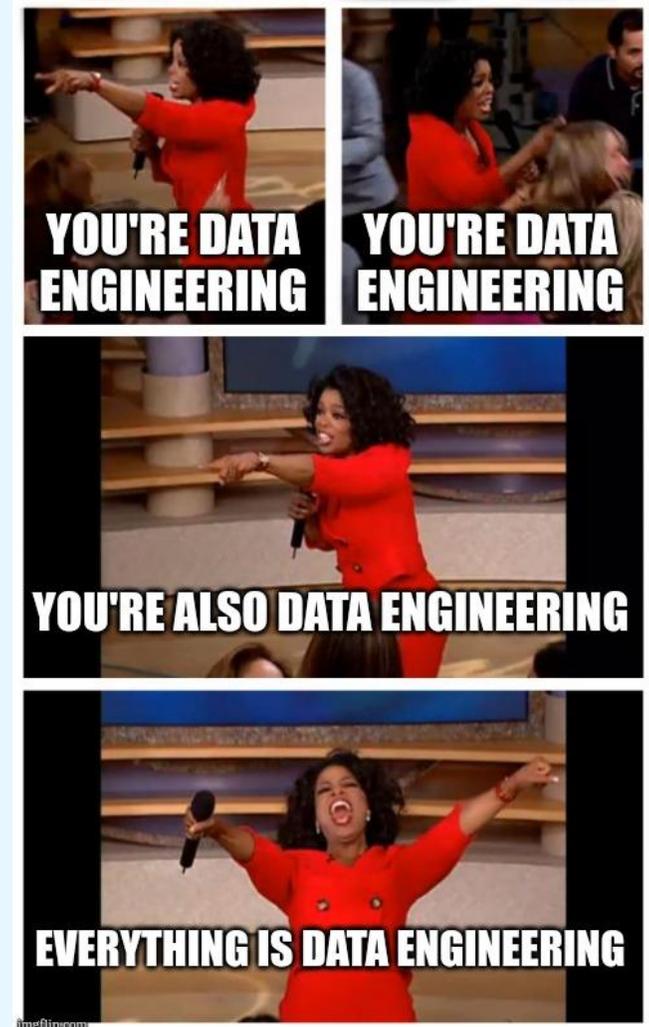
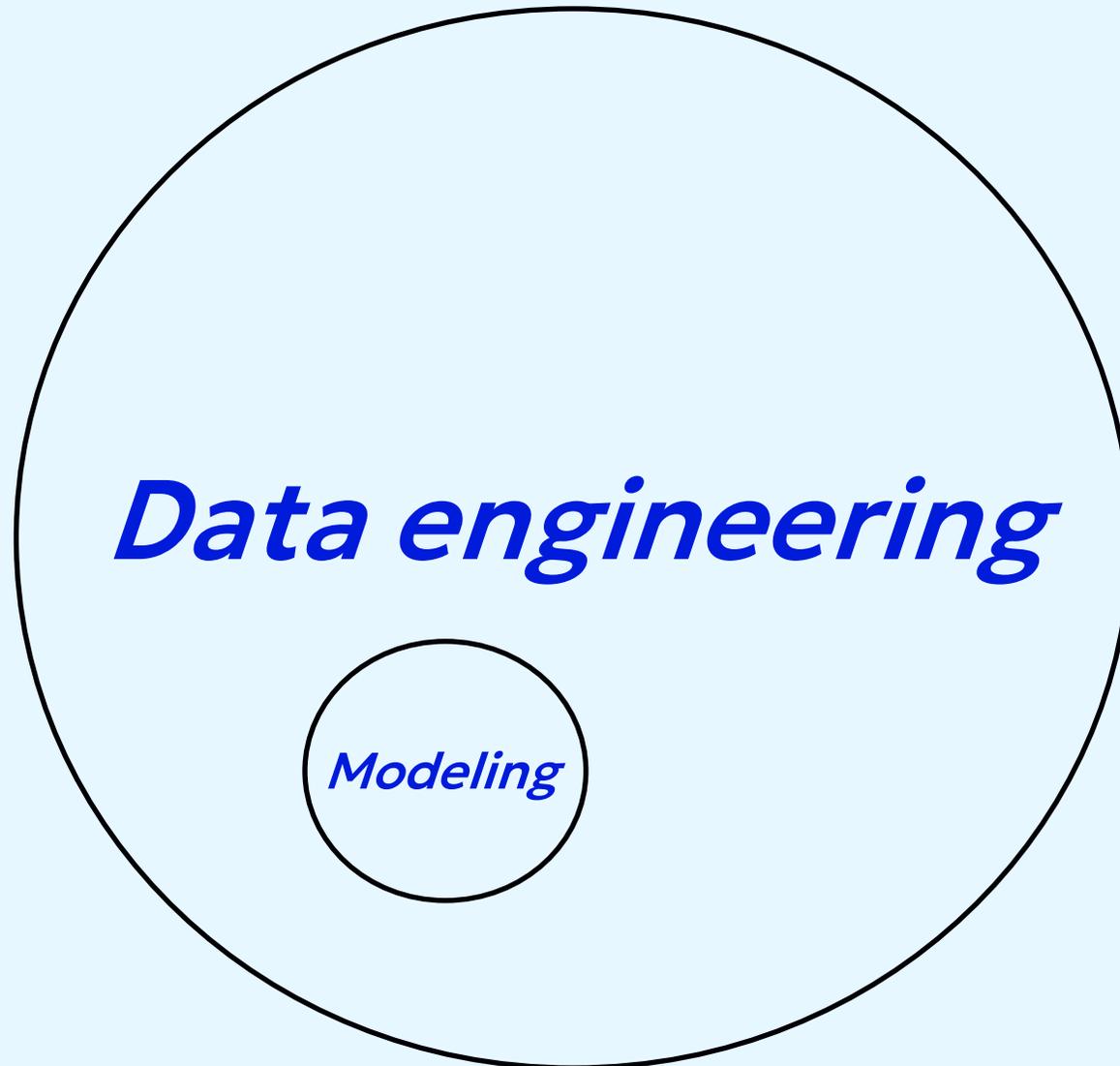
Percieved data landscape



How - Our data landscape



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



oui
nide
iou



3. | OPENCTI

Overview and Demo

OpenCTI Overview



Outputs



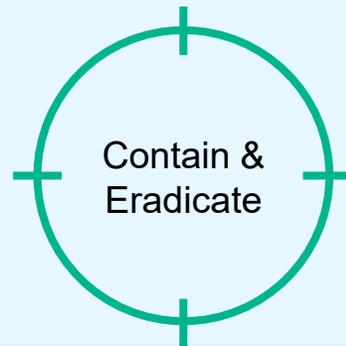
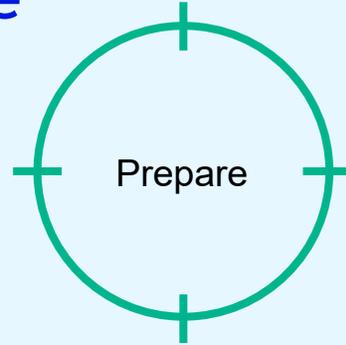
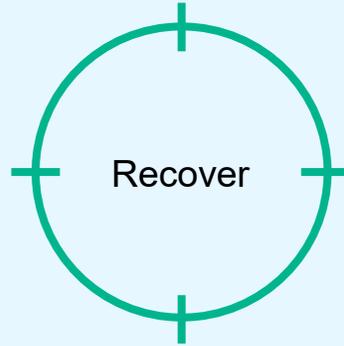


Workflow: Incident Response

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.

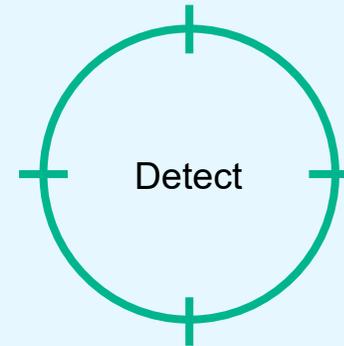
With the help of **RFI**, the decision-maker guides the production of content to guide the recovering process. He can use **notes**. He **can export** investigative content and counter-measures **in .pdf** format or share directly with the right teams.

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.

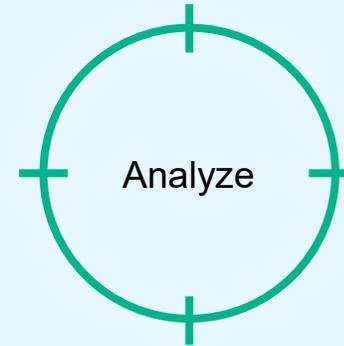


In [OpenCTI](#) :

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.

4. | OPENBAS

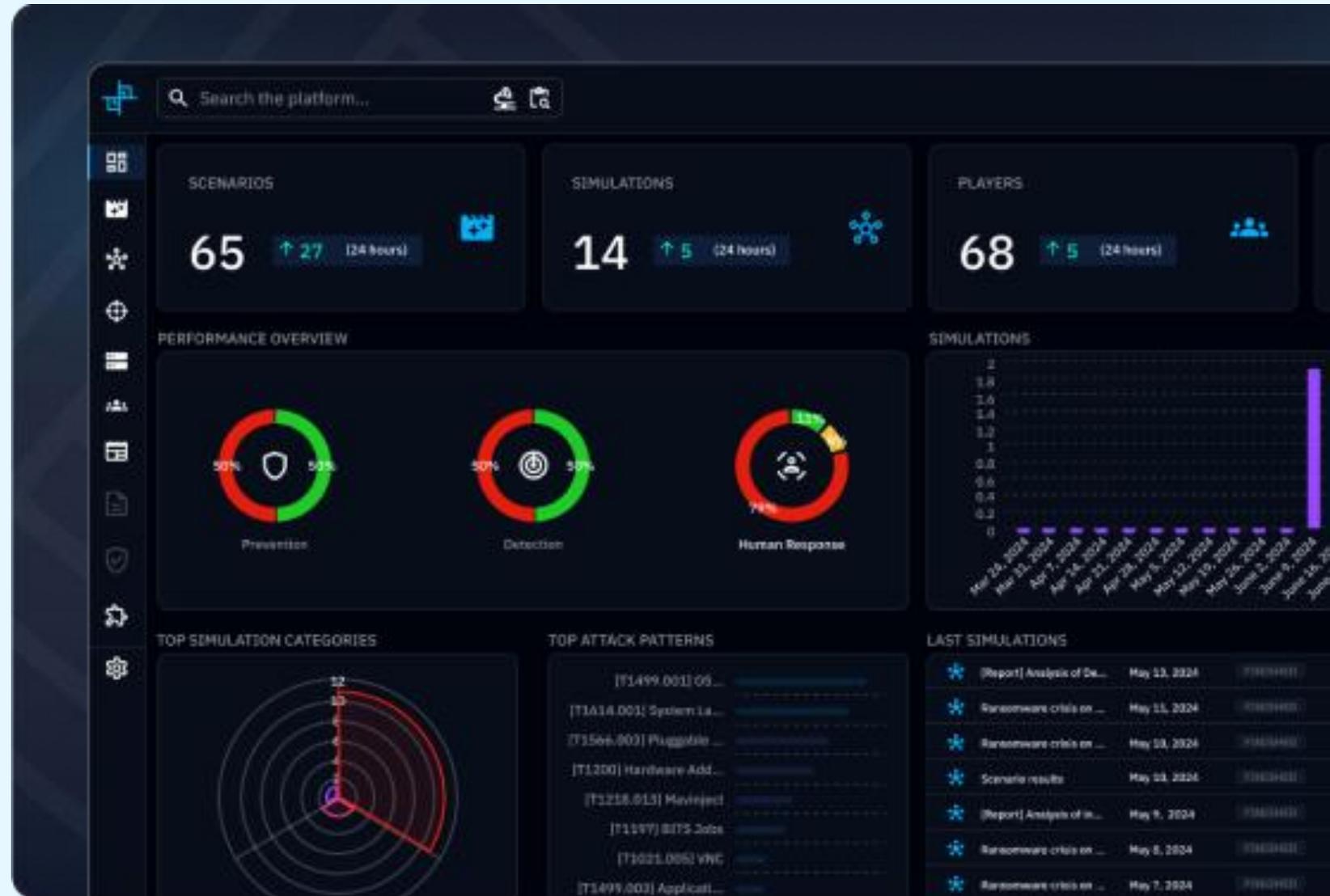
Overview and Demo

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



Akira ransomware

0 SUBSCRIBERS

OVERVIEW KNOWLEDGE CONTENT ENTITIES OBSERVABLES DATA

select-channels-an...	develop-content	command-and-contro...	resource-developme...	privilege-escalati...	impact	target-audience-an...	persistence	execution	develop-narratives	maximiza...
3 techniques	2 techniques	25 techniques	8 techniques	15 techniques	16 techniques	2 techniques	23 techniques	19 techniques	3 techniques	2 te
Formal Diplomatic Channels	Develop Video-Based Content	Application Layer Protocol - T1071	Acquire Access	Account Manipulation - T1098	Account Access Removal	Map Target Audience Information Environment	Account Manipulation - T1098	Cloud Administration Command	Develop Competing Narratives	Cross-Post
Online Pals	Reuse Existing Content	Application Layer Protocol - T1437	Acquire Infrastructure - T1583	Boot or Logon Autostart Execution - T1547	Data Destruction - T1485	test trows	BITS Jobs	Command and Scripting Interpreter	Leverage Existing Narratives	Direct User Platforms
Social Networks		Commonly Used Port	Compromise Accounts - T1586	Boot or Logon Initialization Scripts - T1037	Data Encrypted for Impact - T1471		Boot or Logon Autostart Execution - T1547	Component Object Model and Distributed COM	Respond to Breaking News Event or Active Crisis	
		Communication Through Removable Media	Compromise Infrastructure - T1584	Create or Modify System Process	Data Manipulation - T1565		Boot or Logon Initialization Scripts - T1037	Container Administration Command		
		Content Injection	Develop Capabilities - T1587	Domain or Tenant Policy Modification	Defacement		Browser Extensions	Deploy Container		
		Custom Cryptographic Protocol	Obtain Capabilities - T1588	Escape to Host	Disk Wipe		Compromise Host Software Binary	Exploitation for Client Execution - T1203		
		Data Encroding - T1132	Stage Capabilities - T1608	Event Triggered Execution - T1546	Endpoint Denial of Service - T1499		Create Account - T1136	Graphical User Interface		
		Data Obfuscation - T1001	T1585 - Establish Accounts	Exploitation for Privilege Escalation - T1068	Financial Theft - T1657		Create or Modify System Process	Inter-Process Communication		
		Dynamic Resolution - T1568		Path Interception	Firmware Corruption		Event Triggered Execution - T1546	Native API - T1106		
		Encrypted Channel - T1521		Process Injection - T1055	Network Denial of Service - T1498		External Remote Services - T1133	Scheduled Task/Job - T1053		
		Encrypted Channel - T1973		Scheduled Task/Job - T1053	Not so beautiful TTP		Hypervisor	Scripting		
		Fallback Channels		T1078 - Valid Accounts	Resource Hijacking - T1496		Implant Internal Image	Serverless Execution		
		Hide Infrastructure		T1134 - Access Token Manipulation	Service Stop - T1489		Modify Authentication Process - T1556	Shared Modules - T1129		
		Ingress Tool Transfer - T1105		T1548 - Abuse Elevation	System Shutdown/Reboot - T1529		Office Application Startup	Software Deployment Tools - T1072		
		Ingress Tool Transfer - T1544			T1486 - Data Encrypted For Impact					

Select payloads to inject on your assets



DISABLE MICROSOFT DEFENDER FIREWALL VIA REGISTRY

Disables the Microsoft Defender Firewall for the public profile via registry Caution if you access remotely the host where the test runs! Especially with the cleanup command which will re-enable firewall for the current profile...

Platforms:

Tags: No tag

Attack patterns: [T1562.004] DISABLE OR ...

External ID: afedc8c4-038c-4d82-b3e5-623a95f8a612

Command executor: **cmd**

Attack commands:

```
reg add
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\PublicProfile" /v "EnableFirewall" /t REG_DWORD /d 0 /f
```

Arguments: -

Prerequisites: -

Cleanup executor: **cmd**

Cleanup commands:

```
reg add
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\PublicProfile" /v "EnableFirewall" /t REG_DWORD /d 1 /f
```

Scenarios / Akira Ransomware

Akira Ransomware

OVERVIEW DEFINITION **INJECTS** TESTS LESSONS LEARNED

Search these results... Add filter

Rows per page: 20 1-20

Platforms contains AND Kill chain phase contains AND Injector contains

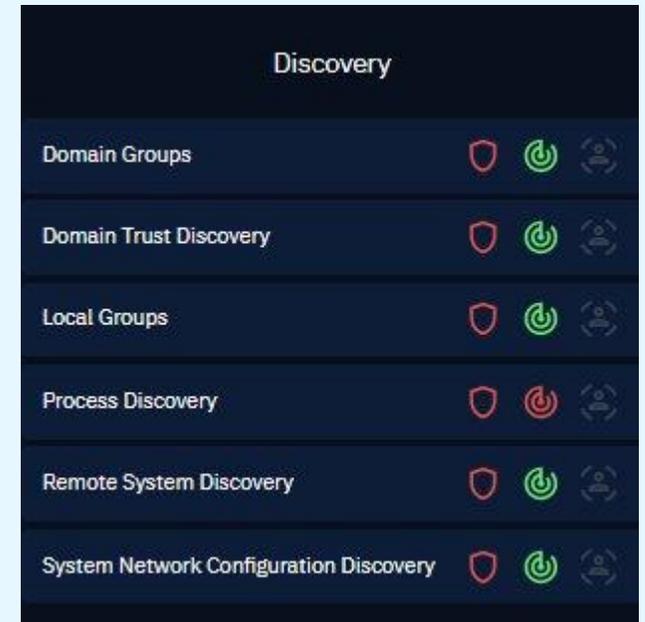
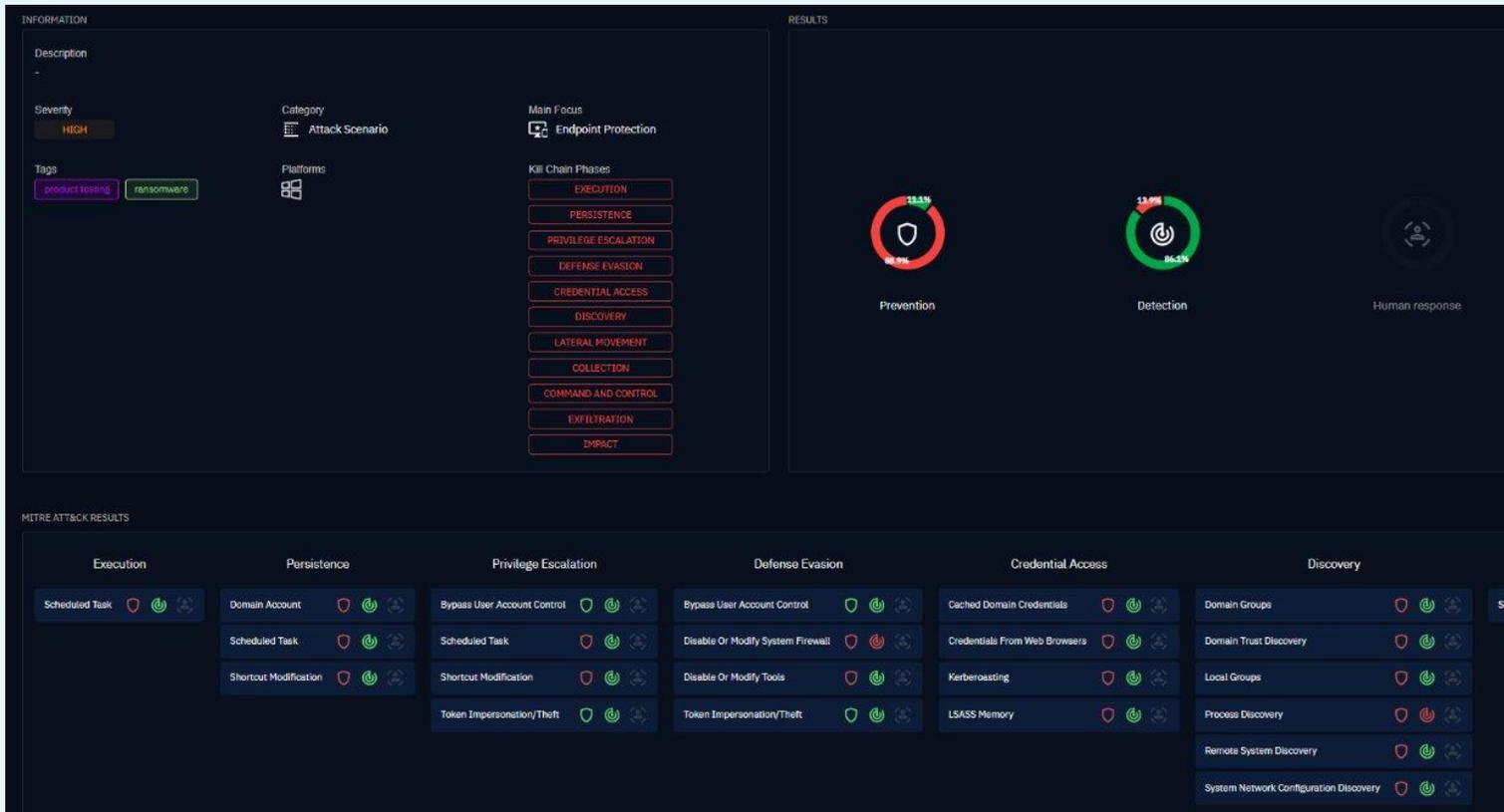
<input type="checkbox"/>	TYPE	TITLE	TRIGGER	PLATFORM(S)	STATUS	TAGS
<input type="checkbox"/>		Windows - Delete V...	Windows - Delete Volume Shadow Copies via WMI with Pow...		ENABLED	No tag
<input type="checkbox"/>		Add 100 Files with ...	Add 100 Files with .akira File Ending + Akira Ransomnote		ENABLED	No tag
<input type="checkbox"/>		PureLocker Ranso...	PureLocker Ransom Note		ENABLED	No tag
<input type="checkbox"/>		Exfiltrate data with ...	Exfiltrate data with rclone to cloud Storage - Mega (Windows)		ENABLED	No tag
<input type="checkbox"/>		Exfiltration Over Alt...	Exfiltration Over Alternative Protocol - FTP - Rclone		ENABLED	No tag
<input type="checkbox"/>		Compress Data for ...	Compress Data for Exfiltration With Rar		ENABLED	No tag
<input type="checkbox"/>		Compress Data and...	Compress Data and lock with password for Exfiltration with ...		ENABLED	No tag
<input type="checkbox"/>		ngrok Proxy Service	ngrok Proxy Service		ENABLED	No tag
<input type="checkbox"/>		AnyDesk Files Dete...	AnyDesk Files Detected Test on Windows		ENABLED	No tag
<input type="checkbox"/>		Disable Microsoft D...	Disable Microsoft Defender Firewall via Registry		ENABLED	No tag
<input type="checkbox"/>		Tamper with Windo...	Tamper with Windows Defender ATP PowerShell		ENABLED	No tag



Get an overview of your security posture



Coming soon



5. | COMMUNITY STORY

Librairie GO

Thank you

Ask us anything



[Filigran.io](https://filigran.io)