



Filigran

Community Meetup

March 2025- Paris

Agenda



1. | OUR LAST NEWS

2. | ROADMAP

3. | OPENCTI DEMO

4. | COMMUNITY USE CASE

5. | Q&A SESSION

1. | OUR LAST NEWS

Filigran Academy, XTM Hub...

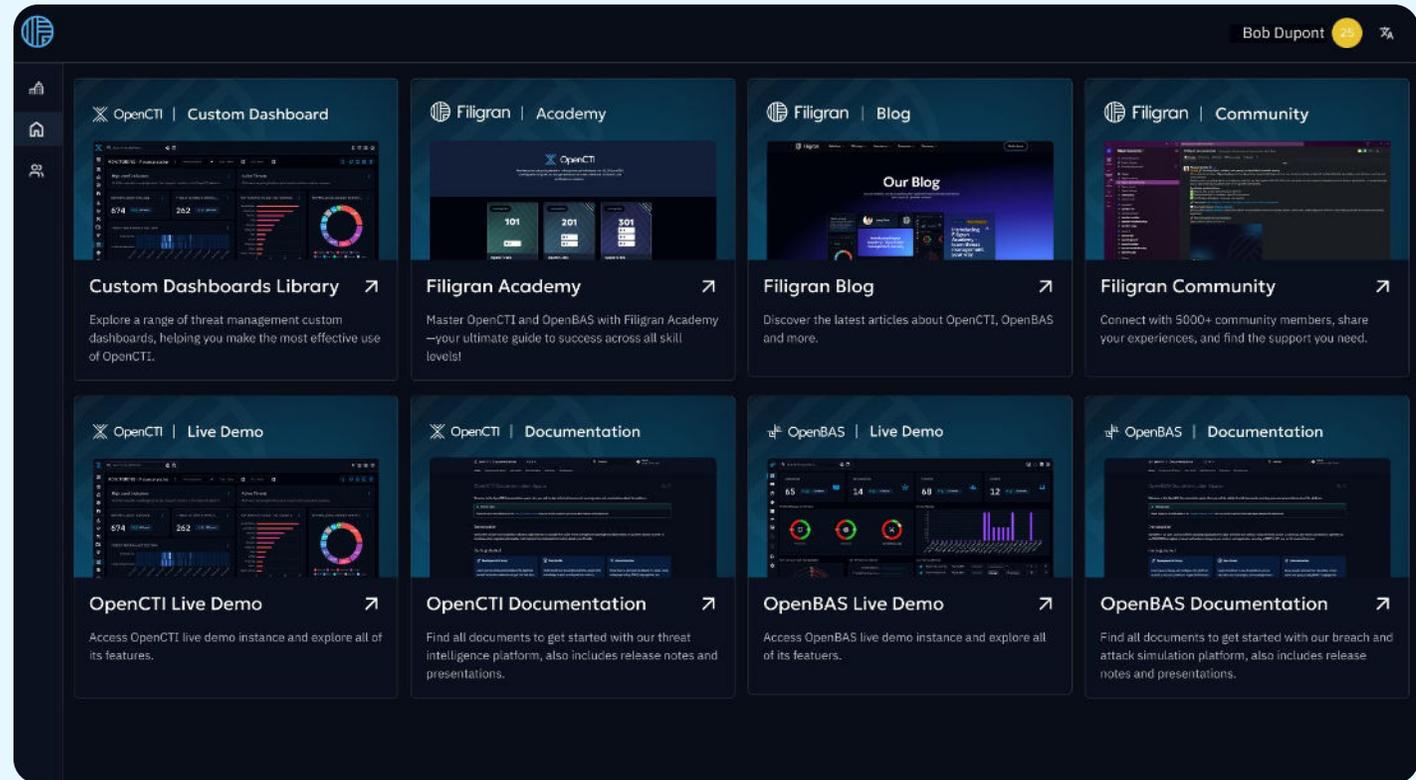
XTM Hub: unified gateway to the Filigran experience



XTM Hub is the **unified entry point** for Filigran's ecosystem.

With just **one registration**, you gain seamless access to product demos, training materials, resources library, and more. No need for multiple logins.

All resources are in one place, making it the ultimate starting point for anyone with Filigran.



XTM Hub: unified gateway to the Filigran experience



XTM Hub is the **unified entry point** for Filigran's ecosystem.

With just **one registration**, you gain seamless access to product demos, training materials, resources library, and more. No need for multiple logins.

All resources are in one place, making it the ultimate starting point for anyone with Filigran.

The focal point to consume every Services and Products



Custom Dashboard library

Access a growing library of pre-built dashboards tailored to specific use cases.



Instant access to live demo instances

Enjoy a streamlined experience to explore OpenCTI and OpenBAS in action.



Direct access to Filigran Academy

Gain direct access to training materials to enhance your skills with our solutions.



Coming soon

Instance monitoring, Playbooks & CSV Mappers library, OpenBAS scenarios library, free trial EE instances...

Introducing Filigran Academy



Filigran Academy is **the all-in-one learning platform** designed to help you master Filigran solutions, including **OpenCTI** and **OpenBAS**.

Through **structured courses, hands-on exercises, and certifications**, it provides an ideal learning path for both beginners or those looking to advance their expertise.



Introducing Filigran Academy



Filigran Academy is **the all-in-one learning platform** designed to help you master Filigran solutions, including **OpenCTI** and **OpenBAS**.

Through **structured courses, hands-on exercises, and certifications**, it provides an ideal learning path for both beginners or those looking to advance their expertise.

Gateway to mastering OpenCTI and OpenBAS:



Tailored learning paths

Follow structured courses designed for all skill levels, from beginners to advanced users.



Hands-on simulations

Apply your knowledge with real-world exercises in a simulated environment.



Certifications and badges

Earn badges and certifications to validate and showcase your expertise.



Flexible learning options

Learn at your own pace with self-service e-learning.

2. | ROADMAP STATUS

What's coming next?

OPENCTI - Features coming next months

Subject to change

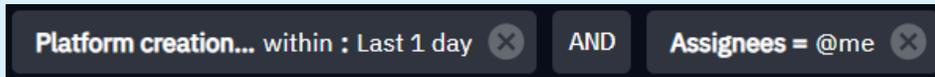
★★ [EE] Natural Language Query



★★ Saved filters

Save/reapply your filters to ease access to the right Intel

★★ “Me” and “relative date-time” filters



★★ Brand new ‘Import from files’ workflow

Import from multiple files, monitor the import status

★★ Draft Workspace

Import/create new data without impacting your validated Intel

★★ [EE] Disseminate intel reports in email body

Include your custom template in your disseminated emails

★★ Priority Intelligence Requirements

Define your PIR and let the platform highlights relevant new data

★★ [EE] Request Access to closed Intel

Request access when you create an entity that already exists

★★ Security Posture definition and assessment

Ready against this threat? Assess continuously with OpenBAS

★★ Connectors composer

Instantiate a connector directly from the UI

★★ Att&ck matrix improvements

Better subtechniques display, matrices overlay, Security gaps

★★ Score for Organizations

Supply chain risks

OPENCTI - Integrations in coming months

Subject to change

★★ ServiceNow

Retrieve incidents from SIR module. Retrieve associated tasks, observables & IOCs

★★ Dragos

Retrieve Dragos Reports and related IoCs

★★ [EE] ImportDocument-AI (NLP model v1)

Extract Threat actors, Malwares and observables even if not already in your platform.

★★ FIRST EPSS import connector FROM COMMUNITY

Update your CVE data with EPSS score from FIRST.

★★ Flashpoint Compromised Credentials Monitoring (CCM)

Retrieve data related to leaked Enterprise credentials

★★ Crowdstrike LogScale

Retrieve SIEM Detections and Incidents and model them as OCTI Incidents and Cases

Verified / Unverified Integrations

Verified = The connector has been fully reviewed by Filigran and can easily be added to your SaaS platform.

UnVerified = The connector has NOT been reviewed by Filigran and cannot yet be used in your SaaS platform. Contact Filigran if you need a connector to be Verified.

OpenCTI Integrations' ecosystem

<https://filigran.notion.site/OpenCTI-Ecosystem-868329e9fb734fca89692b2ed6087e76>

OPENBAS - Features coming next months

Subject to change

★★ Scalable Scenario execution & management

Simulate attacks on 100k+ assets

★★ Ready-to-use High quality Scenario

Repository of Attack Scenarios & Payloads

★★ "Findings" management

Collect dump & output from Payloads. Reuse them.

★★ Customizable Security Posture Dashboards

OpenCTI-like. Create your own KPIs based on OpenBAS data

★★ Proactive alerting and reports

Be Notified when a critical assets is at risk, Security Posture is degraded, etc.

★★ More complex Scenario generation from OpenCTI

IoCs, Artefacts, More precise payloads selection

★★ AI-Assisted Scenario generation

Prompt your Scenario, bootstrap your Scenario in seconds

★★ Remediation path

Get guidance about how to improve your Security Posture

★★ Skillset testing & monitoring

Security Posture is not only about technical appliance & rules

★★ Attack Flow

Security Posture is not only about technical appliance & rules

3. | OPENCTI DEMO

Incident response and investigation

Incident response and investigation



Triage & Correlation

Accelerate incident response by leveraging existing intelligence within the platform for faster and more informed decision-making

Report Production & Sharing

Simplify and accelerate the production and dissemination of your analysis reports

Dashboard

Quickly set up an incident response dashboard, thanks to our XTM Hub dashboard library

4. | LIVE USE CASE

Community Members journey with OpenCTI

How OpenCTI Boosted CTI Detection Efficiency



From Legacy Limits to a New Vision

Understanding the challenges of traditional CTI detection and how a new approach was conceptualized.

Architecture in Action

A technical deep dive into the design, implementation, and workflow of the proposed solution using OpenCTI.

4Y Later: What We Learned

Practical feedback after years of real-world use: benefits gained, problems faced, and lessons learned.

Thank you

Ask us anything



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