



FILIGRAN



Anticipate cyber threats and disrupt crisis preparation

Introduction à Filigran



Présentation

Filigran est une société française de cybertech créé en 2022, qui a pour mission de délivrer aux équipes de cyber sécurité et de gestion de crise, la meilleure des technologies open-source.

La société conçoit et développe un portefeuille de solutions d' **eXtended Threat Management** (XTM), qui couvre la cyber threat intelligence (**Open CTI**), les exercices de simulation à grande échelle (**OpenEx**) et la gestion de crise (**OpenCrisis**).

Filigran sert aujourd'hui des milliers d'organisations privées et publiques à travers le monde.

Filigran – La société



Activités



Cyber Threat Intelligence



Knowledge Management Subsystems



Crisis Management and Preparation



Digital Risk Assessment

Mission et objectifs



Développer des solutions **open-source de haut niveau**



Proposer une alternative SaaS pour ces solutions, à iso-fonctionnalité



Fournir un **support professionnel** et des **éditions “Enterprise”** pour nos produits



Délivrer des **formations** et de la **documentation** détaillée sur nos produits

Identité



Créée en Septembre 2022



30 Employés



Siège social à Paris, France

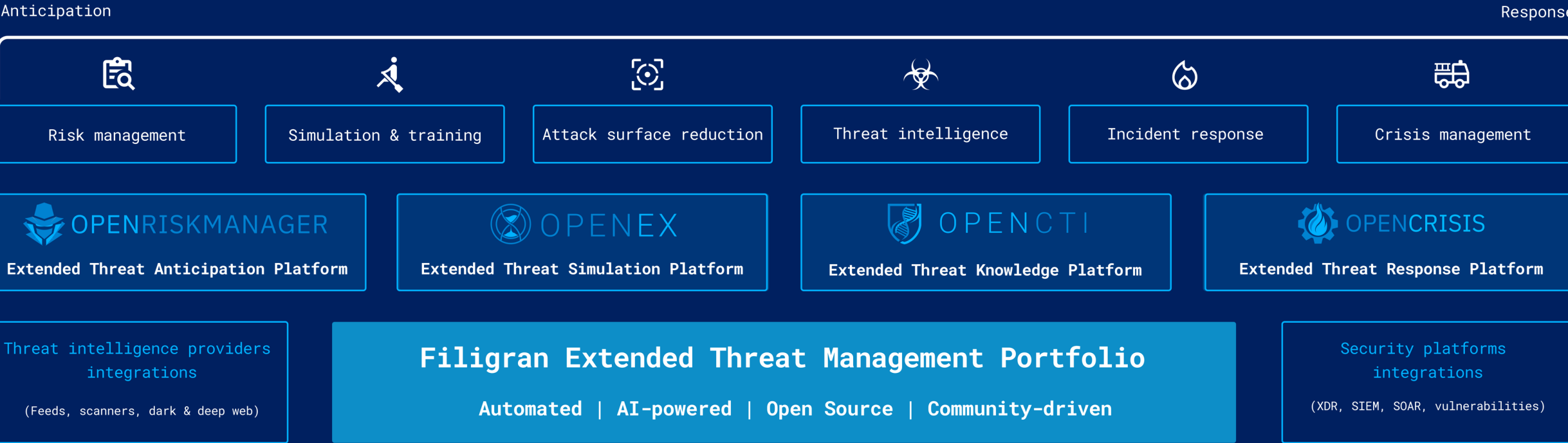


4 000 organisations utilisatrices des solutions Filigran



1ère levée de fonds de 5M€ en Juin 2023

Positionnement : *Extended Threat Management*



Utilisateurs et clients OpenCTI



COMMUNAUTÉ



3 500+

ORGANISATIONS UTILISATRICES



50+

RÉFÉRENCES À L'INTERNATIONAL

TOP PAYS

United States of America
France
United Kingdom
Germany
Australia
Indonesia
Italy
Israel
Brazil

TOP SECTEURS

Public – Defence and Security
Industry – Defence and Security
Consulting – Finance
Consulting - Cybersecurity
Telecom
Consumer Goods
Banking
Hospitality
Public – Local Administrations

CLIENTS



45+

SOUS CONTRAT DE
SUPPORT



20+

SOUS CONTRAT SAAS



Présentation d'OpenCTI

Origine et raison d'être, fonctionnalités principales

Le projet OpenCTI



Origine du projet & raison d'être

- Forte conviction que la communauté CTI manquait d'un outil pour stocker tous les niveaux d'information (opérationnels / stratégiques)
- Nous avons appris de la communauté sur les besoins & attentes des équipes CTI/SOC/DFIR
- Plateforme de gestion de la connaissance Cyber et d'analyses.
- Enrichissements automatiques ou manuels des entités et des observables.
- Gestion unique des doublons par déduplication automatique et fusions des entités.

Cas d'usage

- Cyber Threat Intelligence “Stratégique”
- Cybercriminalité / Renseignement
- Gestion des capacités de détection / “detection-as-code”
- Gestion et modélisation des Incidents
- Evaluation des vulnérabilités
- Campagnes de Threat Hunting et Résultats
- Réduction de la surface d'attaque et Monitoring

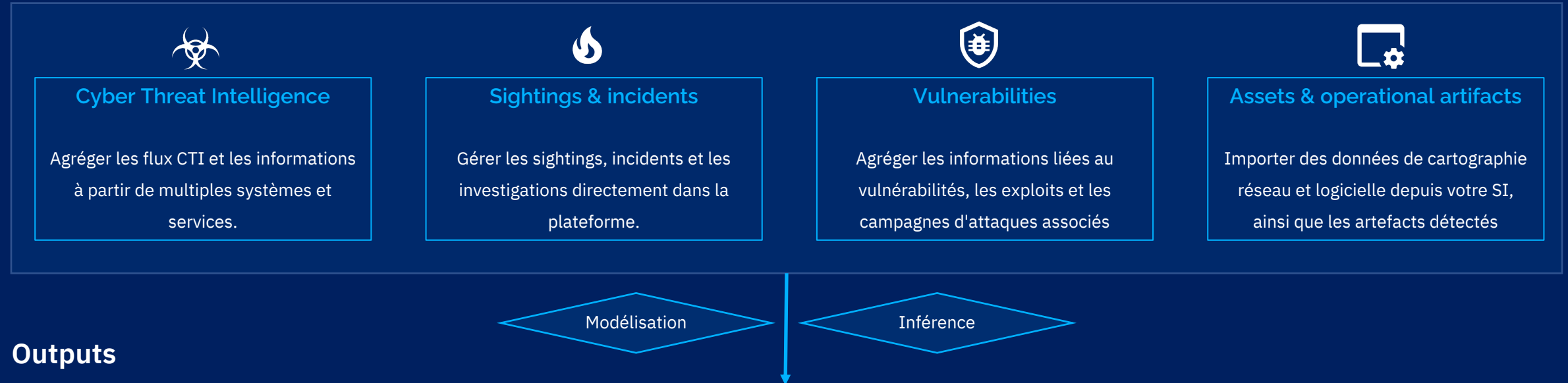
Differentiateurs clés

- Des centaines d'intégrations pour l'alimentation des données, le processing et la diffusion (import, enrichment, export/stream).
- Modèle de données en graphe doté d'un puissant moteur d'inférences, gestion du cycle de vie, règles de rétention , etc.
- Ségrégation avancée des données pour la confidentialité et le partage de connaissance.
- Modèle unifié avec dé-duplication et dashboarding pour une CTI opérationnelle ET stratégique.
- Ecosystème d'intégration Filigran, approche communautaire, open source.

Fonctionnalités principales



Inputs



Outputs



Ecosystème OpenCTI

Connecteurs et integrations

Ecosystème- Inputs



Import data

Ingest Cyber Threat Intelligence and Operational data in OpenCTI.



Import files

Import structured and unstructured files into the platform.



Enrich information

Automatically or on-demand, enrich existing information with external data.



Full catalog

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

Ecosystème – Outputs



File export

Export information to structured and unstructured files.



Streams

Consume the platform streams and push data to third-party systems.



Microsoft Sentinel



Built-in Feeds

Use native feeds capabilities directly from third-party systems to pull data.



Full catalog

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

Présentation d'OpenEx

Fonctionnalités principales

Plateforme OpenEx



Couverture fonctionnelle

- Plateforme de gestion des exercices de simulation de crise cyber, avec interaction entre les joueurs et bilan en fin d'exercice.
- Automatisation des “injects” envoyés aux joueurs ou à des systems externes
- Ecosystème d'intégrations permettant d'envoyer des “injects” à travers une grande variété d'applications tierces
- Simulation de pression médiatique via des informations de sites Web et micro-blogging.
- Interactions avec les joueurs (emails et chat), ajout de fichiers, etc.

Cas d'usage

- Test de la préparation d'une organisation aux attaques cyber
- Retour d'expérience sur les points à améliorer / traiter
- Simulation d'attaque à partir de contributions techniques et opérationnelles
- Réduction de la surface d'attaque
- Simulation de la pression médiatique

Différentiateurs clés

- Simulations combinant les dimensions techniques et stratégiques
- Ecosystèmes ouvert d'injecteurs, pour gérer tout type d'exercices, systems de ticketing et d'alerte, réponse aux incidents
- Templates pour les bilans et “lessons learned” avec attribution de scores
- Interactions multiples intégrées avec les joueurs avec des messages directs, des e-mails, des injections manuelles ou des appels téléphoniques.
- Ecosystème d'intégration Filigran, approche communautaire, open source.



Merci de votre attention

Votre contact Filigran

Antoine Dhillon

Director EMEA

antoine.dhillon@filigran.io

+33 6 31 75 09 20