

Filigran, logiciel open source de renseignements sur les cybermenaces

Description

Développé de manière bénévole depuis 2018 par les Français Samuel Hassine et Julien Richard, le logiciel open source OpenCTI « *fournit des renseignements sur les cybermenaces, des sous-systèmes de connaissances et des solutions de réponse aux crises à des milliers d'équipes de cybersécurité et de gestion des crises dans le monde entier* ». Face au succès d'OpenCTI et pour en assurer le développement, les fondateurs ont créé en octobre 2022 une start-up, Filigran, embauché vingt salariés, et réussi une première levée de fonds de 5 millions d'euros en juin 2023.

L'entreprise évolue dans le domaine du renseignement sur les cybermenaces (en anglais, Cyber Threat Intelligence, CTI). Elle collecte et organise toutes les informations possibles, permettant de dresser le profil des attaquants afin de mieux anticiper les actions, y compris les plus sophistiquées. Samuel Hassine a notamment dirigé le bureau Analyse de la menace et des risques de l'Agence nationale de la sécurité des systèmes d'information (Anssi) de 2015 à 2020. Avec Julien Richard, il développe bénévolement dès 2018 le logiciel OpenCTI, qu'ils lanceront fin 2019. Fait notable, OpenCTI est open source : quiconque peut l'utiliser, avoir accès au code informatique et réaliser des travaux dérivés. Grâce à cette stratégie de l'émancipation vis-à-vis des logiciels propriétaires devenue un enjeu géopolitique ([voir La rem n°64, p.92](#)), Filigran est aujourd'hui utilisé tous les mois par plus de 3 500 organisations dans le monde, parmi lesquelles Airbus, Hermès, SpaceX, Thales, Kaspersky, Bouygues Telecom, tout comme l'Anssi, le ministère des armées, la gendarmerie, la police néerlandaise, et le FBI.

« *Connais-toi, connais ton adversaire, et cent batailles ne te mettront pas en danger* » écrivait Sun Tzu il y a vingt-six siècles dans son ouvrage de stratégie militaire *L'Art de la guerre*. « *Lorsque nous avons publié la première version d'OpenCTI* », expliquaient en 2020 les fondateurs de Filigran sur leur blog, « *nous étions convaincus que la communauté CTI manquait d'un outil efficace pour organiser non seulement les connaissances techniques sur les cybermenaces, mais aussi les TTP [Tactiques, techniques et procédures], la victimologie, les données contextuelles, etc.* ». OpenCTI sert à organiser, de manière simple, l'ensemble des informations et des données relatives aux cybermenaces dont une organisation, un pays ou un secteur de l'économie pourrait être victime, en agrégeant à la fois des flux de données techniques et des informations sur les groupes d'attaquants, sur leurs cyberattaques et même sur leurs tactiques.

« *Concrètement, vous êtes un acteur du luxe, vous avez une présence importante en Chine et vous avez besoin d'identifier les grandes menaces qui peuvent vous cibler ; connaître la météo du risque à l'instant T pour en déduire une feuille de route ; ajuster les priorités d'un point de vue cyber et identifier les tactiques à mettre en place pour se défendre en prenant en compte l'impact business au regard des éventuelles implantations. C'est la proposition de valeur d'Open CTI* » expose Samuel Hassine au site d'information

Maddyness.

Depuis 2021, Filigran développe OpenEx, un deuxième logiciel open source à l'attention des équipes d'analystes et ingénieurs cyber, capable de générer des exercices de gestion de crise et de lancer des campagnes de simulation d'attaque, élaborées à partir des menaces informatiques identifiées grâce à OpenCTI. Un troisième logiciel open source est en cours de développement : OpenCrisis, plateforme ouverte de gestion de crise, dans le feu de l'action et entre plusieurs équipes, pour administrer et centraliser l'organisation d'une réponse à une attaque informatique.

Forts d'une communauté de plus de 3 000 membres et des 3 500 organisations utilisant déjà OpenCTI, les futurs fondateurs de Filigran se rendirent à l'évidence en 2022 : « *Nous arrivons aux limites de l'organisation actuelle, nous avons besoin de nous y consacrer à plein temps et de faire croître l'équipe de recherche et développement tout en développant une entreprise internationale capable de répondre aux enjeux de croissance de nos plateformes* », précise Samuel Hassine à ZDNet.fr. Après avoir converti en clients une trentaine de grands groupes parmi les utilisateurs actifs d'OpenCTI, dont un tiers aux États-Unis et les autres en Europe, la start-up est créée à l'automne 2022 et embauche une vingtaine de personnes. Huit mois plus tard, Filigran lève un fonds d'amorçage de 5 millions d'euros pour structurer une offre commerciale et renforcer la recherche et le développement de leur suite logicielle. Le principal investisseur est le fonds britannique Moonfire Ventures, rejoint par des partenaires financiers importants, notamment Kima Ventures, fonds d'investissement français spécialisé dans le capital d'amorçage et la tech créé en 2010 par Jérémie Berrebi et Xavier Niel ; Motier Ventures, bureau de gestion des investissements des propriétaires du groupe Galeries Lafayette dans les start-up technologiques et CMA CGM Ventures, fonds d'investissement du groupe français CMA CGM, l'un des leaders mondiaux du transport maritime et de la logistique.

De quoi permettre à la start-up, qui table sur un chiffre d'affaires de 3 millions d'euros en 2023 et 7 millions en 2024, de proposer à ses clients un cadre contractuel, notamment pour un accompagnement technique. La suite logicielle, qui restera open source, évoluera, grâce à des investissements majeurs en recherche et développement, vers différents modèles d'intelligence artificielle ainsi que des fonctionnalités de traitement du langage naturel et d'automatisation de traitement de données.

Évolution d'autant plus nécessaire que la concurrence dans le domaine du renseignement sur les cybermenaces est forte, avec des spécialistes déjà bien implantés sur ce marché comme Anomali, créé en 2012 à Redwood City aux États-Unis, et qui a déjà levé 96 millions de dollars, ou encore l'entreprise néerlandaise EclecticIQ, avec 47 millions de dollars de levée de fonds depuis sa fondation en 2014. Estimée à plus de 6 000 milliards de dollars en 2021, la Cyber Threat Intelligence est un commerce en pleine expansion face à l'explosion des dommages liés à la cybercriminalité.

Sources :

- Vitard Alice, « EclecticIQ lève 20 millions d'euros pour optimiser sa plateforme de renseignement sur les cybermenaces », usine-digitale.fr, 1^{er} décembre 2020.

- AFP, « La cybercriminalité a coûté plus de 6 000 milliards de dollars en 2021 », lematin.ch, 10 mai 2022.
- Janvier Théo, « Filigran lève 5 millions d’euros pour ses solutions d’anticipation du risque cyber », journaldunet.com, 13 juin 2023.
- Briant Astrid, « La cybertech s’organise pour lutter contre l’intensification des menaces », maddyness.com, 13 juin 2023.
- Manens François, « De projet bénévole à chouchou des investisseurs, le succès atypique de la pépite cyber Filigran », latribune.fr, 13 juin 2023.
- Marin Jérôme, « Filigran lève 5 millions d’euros pour son « Palantir de la cybersécurité » », usine-digitale.fr, 13 juin 2023.

Categorie

1. Techniques

date créée

29 novembre 2023

Auteur

jacquesandrefines