Filigran, logiciel open source de renseignements sur les cybermenaces

Description

DÃ©veloppÃ© de maniÃ¨re bÃ©nÃ©vole depuis 2018 par les FranÃ§ais Samuel Hassine et Julien Richard, le logiciel open source OpenCTIÂ *Â«Â fournit des renseignements sur les cybermenaces, des sous-systÃ¨mes de connaissances et des solutions de rÃ©ponse aux crises Ã des milliers dâ€™Ã©quipes de cybersÃ©curitÃ© et de gestion des crises dans le monde entierÂ Â»*. Face au succÃ¨s dâ€™OpenCTI et pour en assurer le dÃ©veloppement, les fondateurs ont crÃ©Ã© en octobre 2022 une start-up, Filigran, embauchÃ© vingt salariÃ©s, et rÃ©ussi une premiÃ¨re levÃ©e de fonds de 5Â millions dâ€™euros en juin 2023.

Lâ€™entreprise Ã©volue dans le domaine duÂ renseiÂgnement sur les cybermenacesÂ (en anglais, Cyber Threat Intelligence, CTI).Â 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 sophistiquÃ©es.Â Samuel Hassine a notamment dirigÃ© le bureau Analyse de la menace et des risques de lâ€™Agence nationale de la sÃ©curitÃ© des systÃ¨mes dâ€™information (Anssi) de 2015 Ã 2020. Avec Julien Richard, il dÃ©veloppe bÃ©nÃ©volement dÃ¨s 2018 le logiciel OpenCTI, quâ€™ils lanceront fin 2019. Fait notable, OpenCTI est open sourceÂ : quiconque peut lâ€™utiliser, avoir accÃ¨s au code informatique et rÃ©aliser des travaux dÃ©rivÃ©s. GrÃ¢ce Ã cette stratÃ©gie de lâ€™Ã©mancipation vis-Ã -vis des logiciels propriÃ©taires devenue un enjeu gÃ©opolitique (voirÂ *La remÂ *nÂ°64, p.92),Â Filigran est aujourdâ€™hui utilisÃ© tous les mois par plus de 3Â 500Â organisations dans le monde,Â parmi lesquelles Airbus, HermÃ¨s, SpaceX, Thales, Kaspersky, Bouygues Telecom, tout comme lâ€™Anssi, le ministÃ¨re des armÃ©es, la gendarmerie, la police nÃ©erlandaise, et le FBI.

*Â«Â Connais-toi, connais ton adversaire, et cent batailles ne te mettront pas en dangerÂ Â»*Â Ã©crivait Sun Tzu il y a vingt-six siÃ¨cles dans son ouvrage de stratÃ©gie militaireÂ *Lâ€™Art de la guerre.*Â *Â«Â Lorsque nous avons publiÃ© la premiÃ¨re version dâ€™OpenCTIÂ Â»*, expliquaient en 2020 les fondateurs de Filigran sur leur blog,Â *Â«Â nous Ã©tions convaincus que la communautÃ© CTI manquait dâ€™un outil efficace pour organiser non seulement les connaissances techniques sur les cybermenaces, mais aussi les TTPÂ* [Tactiques, techniques et procÃ©dures]*, la victimologie, les donnÃ©es contextuelles, etc.Â Â»*.Â OpenCTI sert Ã organiser, de maniÃ¨re simple, lâ€™ensemble des informations et des donnÃ©es relatives aux cybermenaces dont une organisation, un pays ou un secteur de lâ€™Ã©conomie pourrait Ãªtre victime,Â en agrÃ©geant Ã la fois des flux de donnÃ©es techniques et des informations sur les groupes dâ€™attaquants, sur leurs cyberattaques et mÃªme sur leurs tactiques.

Â«Â ConcrÃ¨tement, vous Ãªtes un acteur du luxe, vous avez une prÃ©sence importante en Chine et vous avez besoin dâ€™identifier les grandes menaces qui peuvent vous ciblerÂ ; connaÃ®tre la mÃ©tÃ©o du risque Ã lâ€™instantÂ T pour en dÃ©duire une feuille de routeÂ ; ajuster les prioritÃ©s dâ€™un point de vue cyber et identifier les tactiques Ã mettre en place pour se dÃ©fendre en prenant en compte lâ€™impact

business au regard des Ã©ventuelles implantations. Câ€™est la proposition de valeur dâ€™Open CTIÂ Â» Â expose Samuel Hassine au site dâ€™information Maddyness.

Depuis 2021, Filigran dÃ©veloppe OpenEx, un deuxiÃ¨me logiciel open source Ã lâ€™attention des Ã©quipes dâ€™analystes et ingÃ©nieurs cyber, capable de gÃ©nÃ©rer des exercices de gestion de crise et de lancer des campagnes de simulation dâ€™attaque, Ã©laborÃ©es Ã partir des menaces informatiques identifiÃ©es grÃ¢ce Ã OpenCTI. Un troisiÃ¨me logiciel open source est en cours de dÃ©veloppementÂ : OpenCrisis, plateforme ouverte de gestion de crise, dans le feu de lâ€™action et entre plusieurs Ã©quipes, pour administrer et centraliser lâ€™organisation dâ€™une rÃ©ponse Ã une attaque informatique.

Forts dâ€™une communautÃ© de plus de 3Â 000Â membres et des 3Â 500Â organisations utilisant dÃ©jÃ OpenCTI, les futurs fondateurs de Filigran se rendirent Ã lâ€™Ã©vidence en 2022Â :Â *Â«Â Nous arrivons aux limites de lâ€™organisation actuelle, nous avons besoin de nous y consacrer Ã plein temps et de faire croÃ®tre lâ€™Ã©quipe de recherche et dÃ©veloppement tout en dÃ©veloppant une entreprise internationale capable de rÃ©pondre aux enjeux de croissance de nos plateformesÂ Â»*, prÃ©cise Samuel Hassine Ã ZDNet.fr. AprÃ¨s avoir converti en clients une trentaine de grands groupes parmi les utiliÂsateurs actifs dâ€™OpenCTI, dont un tiers aux Ã‰tats-Unis et les autres en Europe,Â la start-up est crÃ©Ã©e Ã lâ€™automne 2022 et embauche une vingtaine de personnes. Huit mois plus tard, Filigran lÃ¨ve un fonds dâ€™amorÃ§age de 5Â millions dâ€™eurosÂ pour structurer une offre commerciale et renforcer la recherche et le dÃ©veloppement de leur suite logicielle. Le principal investisseur est le fonds britannique Moonfire Ventures, rejoint par des partenaires financiers importants, notamment Kima Ventures, fonds dâ€™investissement franÃ§ais spÃ©cialisÃ© dans le capital dâ€™amorÃ§age et la tech crÃ©Ã© en 2010 par JÃ©rÃ©mie Berrebi et Xavier NielÂ ; Motier Ventures, bureau de gestion des investissements des propriÃ©taires du groupe Galeries Lafayette dans les start-up technologiques et CMA CGM Ventures, fonds dâ€™investissement du groupe franÃ§ais CMA CGM, lâ€™un des leaders mondiaux du transport maritime et de la logistique.

De quoi permettre Ã la start-up, qui table sur un chiffre dâ€™affaires de 3Â millions dâ€™euros en 2023 et 7Â millions en 2024, de proposer Ã ses clients un cadre contractuel, notamÂment pour un accompagnement technique.Â LaÂ suite logicielle, qui restera open source, Ã©voluera, grÃ¢ce Ã des investissements majeurs en recherche et dÃ©velopÂpement,Â vers diffÃ©rents modÃ¨les dâ€™intelligence artificielle ainsi que des fonctionnalitÃ©s de traitement du langage naturel et dâ€™automatisation de traitement de donnÃ©es.

Ã‰volution dâ€™autant plus nÃ©cessaire que la concurrence dans le domaine du renseignement sur les cybermenaces est forte, avec des spÃ©cialistes dÃ©jÃ bien implantÃ©s sur ce marchÃ© commeAnomali, crÃ©Ã© en 2012 Ã Redwood City aux Ã‰tats-Unis, et qui a dÃ©jÃ levÃ© 96Â millions dedollars, ou encore lâ€™entreprise nÃ©erlandaise EclecticIQ, avec 47Â millions de dollars de levÃ©e defonds depuis sa fondation en 2014. EstimÃ©e Ã plus de 6Â 000Â milliards de dollars en 2021,Â la CyberThreat Intelligence est un commerce en pleine expansion face Ã lâ€™explosion des dommages liÃ©s Ã la cybercriminalitÃ©.

SourcesÂ :

- Vitard Alice, Â« EclecticIQ lÃ¨ve 20 millions dâ€™euros pour optimiser sa plateforme de renseignement sur les cybermenaces Â», usine-digitale.fr, 1er dÃ©cembre 2020.
- AFP, Â« La cybercriminalitÃ© a coÃ»tÃ© plus de 6 000 milliards de dollars en 2021 Â», lematin.ch, 10 mai 2022.
- Janvier ThÃ©o, Â« Filigran lÃ¨ve 5 millions dâ€™euros pour ses solutions dâ€™anticipation du risque cyber Â», journaldunet.com, 13 juin 2023.
- Briant Astrid, Â« La cybertech sâ€™organise pour lutter contre lâ€™intensification des menaces Â», maddyness.com, 13 juin 2023.
- Manens FranÃ§ois, Â« De projet bÃ©nÃ©vole Ã chouchou des investisseurs, le succÃ¨s atypique de la pÃ©pite cyber Filigran Â», latribune.fr, 13 juin 2023.
- Marin JÃ©rÃ´me, Â« Filigran lÃ¨ve 5 millions dâ€™euros pour son Â«Â Palantir de la cybersÃ©curitÃ©Â Â» Â», usine-digitale.fr, 13 juin 2023.Â

Categorie

1. Techniques

date crÃ©Ã©e
29 novembre 2023
Auteur
jacquesandrefines