# Sécurité : « Depuis 2012, l'hyper-automatisation est une priorité » (Laurent Oudot, Tehtris)

La jeune pousse française, fondée il y a une dizaine d'années par Eléna Poincet et Laurent Oudot, a récemment levé 20 millions d'euros et est entrée dans une phase de croissance accélérée. Son cofondateur et directeur technique explique l'approche globale et automatisée qui anime l'entreprise.

Par Valéry Marchive

**LEMAGIT** : Lors de notre première rencontre, il y a bientôt trois ans, Tehtris proposait déjà une offre étendue sous la gamme eGambit, avec EPP/EDR, MTD, SIEM, ou encore IDS – notamment. Comment s'articule aujourd'hui votre offre ?

**LAURENT OUDOT**, co-fondateur et directeur technique de Tehtris : Notre vision est la même depuis la création en 2012, à savoir proposer une plateforme holistique afin de protéger les systèmes et les réseaux informatiques sans angle mort.
Mes discussions avec les analystes de Gartner ont confirmé, il y a un an et demi, la nécessité de créer une plateforme unifiée qui regrouperait EDR, EPP, SIEM, Honeypot, MTD et SOAR, dans laquelle l'intelligence artificielle permettrait une hyperautomatisation pour une protection toujours plus étendue. De là est née la plateforme eXtended Detection and Response, que vous

connaissez sous l'acronyme XDR. Notre eGambit originel est devenu la Tehtris XDR Platform. Il est clé de rappeler qu'originellement nous étions les premiers à proposer cette technologie et encore aujourd'hui elle est la seule XDR européenne native offrant ainsi une vue unifiée sur tous les terminaux de nos utilisateurs.

Tout est prévu pour que le déploiement soit rapide et facile, pour que les modules interagissent ensemble et s'imbriquent avec les outils déjà mobilisés grâce à notre SOAR intégré.

Laurent Oudot, Tehtris

L'exigence de protection et de souveraineté nous a conduit naturellement à héberger les données en Europe, ce qui nous permet de positionner Tehtris en tiers de confiance sur les systèmes des entreprises ou des administrations souvent, et hélas encore trop, équipés de logiciels étrangers.

La R&D est très active au sein de notre direction technique dans cette optique d'accroître toujours plus la sécurité et la prise en main de nos clients et partenaires.

Parmi les nouveaux modules, la grande innovation 2020 fut notre MTD sur iOS. Encore une fois, nous étions les premiers à proposer une telle protection des iPhone et iPad, et je vous invite à consulter le Market Guide « *Mobile Threat Defense* » de Gartner qui nous cite comme référence. Sont également mis sur le marché un DNS Firewall ainsi qu'un module de Zero Trust Response : de la haute couture française, entièrement construite par Tehtris.

**« Nous sommes en train de devenir un tiers de confiance européen, déployable pour protéger les données et les activités des entreprises et des administrations, contre le cybersabotage et le cyberespionnage. »**

*- Laurent Oudot, Tehtris*

**LEMAGIT** : Vous avez reçu un fort investissement en début d'année. Comment avez-vous trouvé l'énergie et les ressources pour réaliser tous ces nouveaux développements en seulement trois ans ?

**LAURENT OUDOT** : Notre culture et nos valeurs ont attiré de nombreux talents ces trois derniers mois où plus de 85 personnes ont ainsi été recrutées. Notre mission et nos convictions nous ont menés ici et nous portent collectivement pour le futur.

Nous sommes en train de devenir un tiers de confiance européen, déployable pour protéger les données et les activités des entreprises et des administrations, contre le cybersabotage et le cyberespionnage.

Pendant 10 ans, nous avons autofinancé l'activité, en réinvestissant directement les succès commerciaux dans nos priorités de R&D. Fin 2020 a été officialisée notre levée de fonds de 20 millions d'euros, un record pour une série A en cybersécurité qui contribue à sa mesure au rayonnement de la French Tech.

Au-delà de la somme conséquente qui est d'une précieuse aide pour le développement ambitionné, nous désirions surtout nous engager dans une relation de confiance et de partenariat avec des investisseurs européens. Challenge réussi ! Aujourd'hui et demain pour faire vibrer la France et l'Europe, nous avons parfaitement conscience qu'il faut fédérer les générations, continuer sans cesse d'innover, devenir une force commerciale incontournable et travailler de pair avec nos partenaires et les politiques publiques.

**LEMAGIT** : Quels sont les défis techniques de consolidation de vos différentes briques logicielles au sein de votre offre dite XDR ?

**LAURENT OUDOT** : Depuis 2012 et notre premier produit l'eGambit, l'hyperautomatisation est une priorité. C'est une évidence, quand on observe la croissance exponentielle des attaques cyber et la prise de conscience généralisée de l'état des vulnérabilités.

> **« L'ensemble est orchestré et consolidé par le Tehtris SOAR. »**
>
> *- Laurent Oudot, Tehtris*

Tous les modules de la Tehtris XDR Platform ont été développés en interne. L'équipe a donc naturellement pris en compte les synergies et communications automatisées entre les produits et notre Tehtris CTI (Cyber Threat Intelligence). L'ensemble est orchestré et consolidé par le Tehtris SOAR. Tehtris XDR Platform peut aujourd'hui se déployer en 10 minutes, un temps record, pour offrir des services dans le monde entier. Actuellement, nous sommes déployés dans une centaine de pays.

**LEMAGIT** : Pour vos clients, qu'implique l'adoption de votre offre XDR, que ce soit en termes de déploiements en local ou de gestion des flux de télémétrie ?

**LAURENT OUDOT** : Selon les besoins des clients, nous proposons la Tehtris XDR Platform sous forme d'offre SaaS, on-premise ou hybride. Dans le deuxième cas, après échanges avec le client et spécification de ses

besoins, nous lui fournissons les éléments à télécharger et nous lui mettons en place la ou les machines virtuelles adaptées. Un exemple de simplicité : plus de 10 000 agents EDR déployés et plusieurs SIEM on-premise dans une multinationale en proie à une affaire d'espionnage international, en moins d'une semaine, là où des projets standards classiques mettraient des mois, tout cela grâce à l'automatisation et la simplification de la gestion des flux de télémétrie.

Et d'ailleurs, la gestion de tous les flux est assez simple et hautement sécurisée, puisque tout est chiffré de bout en bout. D'un point de vue client, cela se matérialise par du paramétrage.

**LEMAGIT** : Comment gérez-vous, d'une part, les exigences de confidentialité de vos clients et, d'autre part, la consolidation d'une threat intelligence prête à consommer pour ceux qui en sont clients – uniquement ou dans le cadre d'une offre plus large ?

**LAURENT OUDOT** : Il y a une vraie problématique de confidentialité sur le marché des XDR, cela devrait d'ailleurs être un critère de choix majeur parmi les solutions existantes… si les entreprises désirent rester maîtresses et possesseuses de leurs données.

L'épée de Damoclès qu'est le CLOUD Act, auquel les

entreprises américaines sont soumises, n'est un secret pour personne. Nos data centers sont bien évidemment localisés au sein de l'Union européenne ou dans le pays demandé par le client pour ses problématiques juridiques et stratégiques comme en Chine, en Suisse, etc.

Très concrètement, la grande majorité des EDR ou des XDR sur le marché donne aux analystes SOC ou CERT un accès complet et sans limites aux données des postes de travail et des serveurs. Dans ce contexte, qui empêchera un cyberanalyste d'avoir accès aux budgets d'une entreprise ou à des secrets d'État ? Il est très dangereux de choisir un garde du corps qui peut vous impacter négativement.

**« Les analystes qui utilisent la Tehtris XDR Platform effectuent leur veille et garantissent l'innocuité des fichiers, mais ils ne peuvent pas les consulter. »**

*- Laurent Oudot, Tehtris*

J'évoquais un peu plus haut la notion de confiance : chez Tehtris nous savons (et nous le faisons) qu'il est possible de développer un EDR ou une XDR respectant la confidentialité et la propriété intellectuelle du client.

La notion d'éthique est au cœur de nos valeurs. Aussi, les analystes qui utilisent la Tehtris XDR Platform effectuent leur veille et garantissent l'innocuité des fichiers, mais ils ne peuvent pas les consulter. La sécurité ? Oui. Le vol de données simplifiées à cause de la sécurité ? Non.

Autre exemple encore plus critique, nos machines virtuelles sont parmi les seules au monde à avoir le disque dur 100 % chiffré, « *full disk encryption* », alors que certains SIEM ou EDR concurrents laissent les données en clair – avec les risques de sécurité que cela induit. Les données qui nous intéressent sont celles sur les menaces, pas celles de nos clients.

Ensuite notre vivante Cyber Threat Intelligence alimente au quotidien la consolidation de plusieurs de nos sources et l'efficacité de nos outils, et de fait le degré de sécurité de nos clients.

**LEMAGIT** : Outre vos produits, vous proposez des services, notamment de SOC managé. Quel est le profil des organisations ayant aujourd'hui recours à un tel service ? Et pour quel type d'organisation pensez-vous qu'il est raisonnable de ne pas y avoir recours, et de se contenter d'adopter vos produits ?

**LAURENT OUDOT** : Nous avons différents types de clients : ceux disposant de leur propre SOC, ceux qui choisissent

d'utiliser nos solutions de manière hyperautomatisée et ceux qui choisissent de confier leur SOC à l'un de nos partenaires. Le choix dépend principalement de la taille du client ainsi que de celle de son équipe de sécurité informatique. Les critères tels que l'aversion au risque entrent également en jeu. Du côté produit, nous avons pensé la Tehtris XDR Platform de façon hyperpersonnalisable pour convenir à tous les contextes et répondre à l'ensemble des besoins.

La plupart de nos nouveaux clients accompagnent l'utilisation de leur Tehtris XDR Platform d'un contrat de SOC managé. De plus, en 2019, nous avons accentué notre ancrage en tant qu'éditeur de logiciels, renforçant notre volonté de travailler en collaboration avec des partenaires. Cette stratégie est porteuse, et nous évoluons aujourd'hui avec Capgemini Sogeti, Orange Cyber Defense, Expleo et Cybersec&You.

**LEMAGIT** : Aujourd'hui, comment se répartissent vos effectifs et dans quels domaines cherchez-vous en priorité à recruter ?

**LAURENT OUDOT** : Tehtris, c'est aujourd'hui 140 personnes, dont 100 au sein de la direction technique. Les équipes R&D, les développeurs et les analystes représentent donc 70 % de l'effectif total. Nous avons cette année encore une trentaine de postes ouverts dans ces équipes d'experts techniques. Cet article peut-être une bonne occasion pour faire un appel : nous recherchons des experts en développement logiciel, avec des compétences en Python, Rust et C++.

Notre priorité reste tournée vers l'innovation autour de solutions à la pointe de la technologie afin de désarmer les cyberattaquants et de contribuer à la cyberpaix dans le monde. ■

**VALÉRY MARCHIVE**, *rédacteur en chef du MagIT et responsable éditorial de « Information sécurité ».*