TEHTRIS : des solutions de cybersécurité hyper automatisées et 100 % Made In France

La criticité de la cybermenace est aujourd'hui connue de tous. L'enjeu pour les entreprises est non seulement de pouvoir s'équiper avec des solutions technologiques efficaces, mais également souveraines dans un monde où la cybersécurité n'est plus seulement une question technique, mais également un enjeu business. *Explications d'Ingrid Söllner, Chief Marketing Officer de TEHTRIS, la seule entreprise européenne à proposer une plateforme XDR souveraine.*

Ingrid Söllner

Au cours des dernières décennies la cybersécurité est devenue une préoccupation majeure des entreprises. Pourquoi ?

Nous sommes face à une recrudescence des attaques qui sont devenues plus sophistiquées au fil des années. La médiatisation de ce phénomène et le recours croissant au télétravail ont contribué à placer la cybersécurité au cœur de toutes les préoccupations. Selon une étude Gartner, 88 % des dirigeants d'entreprises déclarent que la cybersécurité est un risque business. Il ne s'agit plus uniquement d'un sujet qui relève de la direction IT, mais d'un enjeu au niveau de la direction générale des entreprises. En effet, une cyberattaque peut bloquer l'activité d'une entreprise, mais également fortement nuire à son image et à la relation de confiance qu'elle entretient avec ses clients, ses prestataires et ses partenaires. Malgré cette prise de conscience, la cybersécurité est encore perçue par certaines entreprises comme un investissement et un coût alors qu'il s'agit pour l'entreprise d'un moyen d'anticiper, d'éviter une attaque.

En parallèle, on note un réel déficit en ressources humaines dans ce domaine. Entre 2013 et 2021, le nombre de postes à pourvoir en cybersécurité a augmenté de 350 %. Faciliter la surveillance des systèmes et réagir en temps réel, c'est la force de la plateforme TEHTRIS, alliée des équipes de sécurité.

En termes de risques, quels sont les principaux risques auxquels sont exposées les entreprises aujourd'hui ?

Les risques opérationnels sont le sabotage de l'activité et l'espionnage. À ceux-ci s'ajoutent des risques financiers, juridiques, réputationnels (comme indiqué précédemment)… et potentiellement des atteintes à la survie de l'entreprise. Ils se matérialisent le plus souvent par une intrusion dans les systèmes. Cliquer par erreur sur un lien ou bien télécharger un fichier malveillant reste la principale porte d'entrée d'une attaque. Cela représente encore plus de 80 % des intrusions qui impliquent un ransomware. D'autres techniques permettront aux cyberattaquants d'entrer dans le système de l'entreprise comme l'exploitation de vulnérabilités dans les programmes, l'usurpation d'identité ou l'ingénierie sociale, c'est-à-dire des actions visant à trouver des informations sur un dirigeant, ses mots de passe, etc.

Personne n'est à l'abri de ces attaques. Toutes les entreprises, de toutes tailles et tous secteurs, sont des cibles potentielles. Dès lors qu'un système informatique est connecté, il s'expose aux menaces et à l'ingéniosité des attaquants.

Dans ce cadre, quels sont les principaux besoins des entreprises ?

Pour faire face aux incidents, les maîtriser et y répondre, chaque entreprise doit connaître l'état de ses systèmes, réseaux et cloud. Les dirigeants l'ont bien compris et appliquent en général des mesures de stricte limitation des accès, d'authentification forte et de sensibilisation de leurs équipes sur différents sujets critiques : la gestion des mots de passe et des accès, la vigilance quant aux téléchargements de fichiers malveillants ou l'accès à des liens servant à faire du phishing…

Les organisations doivent aussi déployer une stratégie de protection de leurs données en s'assurant de réaliser régulièrement des sauvegardes, tout en faisant en sorte de ne pas stocker l'ensemble de leurs données au même endroit.

Il est aussi très important de disposer des moyens et des capacités requis pour pouvoir

réagir en temps réel. Pour ce faire, elles doivent miser sur l'automatisation pour alléger et simplifier le travail des équipes qui surveillent les parcs informatiques avec des technologies capables de bloquer les attaques en temps réel. Et c'est justement sur ces sujets que TEHTRIS a développé une expertise et une expérience avérées.

Et dans cet environnement, quelle est la valeur ajoutée de vos solutions ?

TEHTRIS est un éditeur français de solution de cybersécurité. Nous avons développé une plateforme eXtended Detection & Response (XDR Platform) 100 % native qui fait de la détection et de la réponse aux attaques. Concrètement, notre plateforme identifie et neutralise les menaces connues et inconnues en temps réel et en s'appuyant sur une technologie développée en France.

En effet, en matière de cybersécurité, orchestrer les événements et réagir aux menaces rapidement et avec efficacité est un enjeu fondamental. Pour relever ce challenge, nous capitalisons sur l'intelligence artificielle avec du machine learning et du deep learning, pour doter nos solutions d'une puissante hyper automatisation. Notre outil Security Orchestration Automation and Response (SOAR) embarqué dans la TEHTRIS XDR Platform permet de gérer les différentes API internes et natives qui sont utilisées entre nos produits, comme EDR (Endpoint Detection and Response), EPP (antivirus nouvelle génération), SIEM (Security Information and Event Management), mais aussi les antivirus de nos clients. Cette coordination et cette fluidité de l'action permet de neutraliser en temps réel les cyber-menaces.

En outre, nous répondons aux besoins des entreprises et des administrations avec des offres dimensionnées en fonction de leur taille et de leurs besoins.

Nous avons aussi développé des partenariats technologiques afin de compléter notre offre de sécurité. Par exemple, avec Proofpoint, nous collaborons sur la sécurisation des e-mails, un des principaux vecteurs d'attaque. Ces partenariats permettent à nos clients de conserver leurs solutions de sécurité et de les interfacer avec nos solutions sans investissements supplémentaires. Cela permet, en plus, d'optimiser la remontée des alertes et de permettre une réponse en temps réel. Cette complémentarité vient aussi renforcer l'écosystème cybersécurité et contribue à la lutte contre les attaquants.

“Nous avons développé une plateforme eXtended Detection & Response (XDR Platform) 100 % native qui fait de la détection et de la réponse aux attaques. Concrètement, notre plateforme identifie et neutralise les menaces connues et inconnues en temps réel et en s'appuyant sur une technologie développée en France.”

Enfin, nous hébergeons les données de nos clients en Europe et garantissons leur sécurisation sans accéder aux contenus. Là où nos concurrents vont télécharger un fichier pour le vérifier, nous ne rentrons jamais dans les fichiers de nos clients et garantissons la confidentialité de leurs données.

Au-delà vous contribuez aussi à la souveraineté européenne et française sur ces sujets. En quoi est-ce une garantie supplémentaire ?

Notre code a été intégralement et nativement développé en interne et en France. C'est une solution 100 % made in Europe. Nos modules ont ainsi d'emblée été pensés pour communiquer entre eux. Et si l'un d'entre eux est mis à jour, les autres se mettent à jour automatiquement. Cela garantit, en plus, une unité dans le produit !

Comme précédemment mentionné, l'hébergement est fait en Europe. Cela protège les données que nous stockons des lois extraterritoriales comme le Cloud Act. Enfin, nous créons de la valeur et de l'emploi hautement qualifié en France. En octobre 2020, nous étions 50 personnes. Nous sommes aujourd'hui plus de 200 personnes ! Nous recrutons encore et contribuons, en tant que mécènes, à former les ingénieurs de demain.