3 questions à Jacques de La Rivière

Président co-fondateur de Gatewatcher

➔ SDBR : En 2 ans, vous avez initié une vraie « success story ». Quel en est le secret ?

Jacques de La Rivière* : Gatewatcher** est la 1ère solution de détection des intrusions avancées (Breach Detection System), 100% développée en France et répondant aux exigences de durcissement émises par l'ANSSI, conformément à la Loi de Programmation Militaire. C'est sans doute l'une des raisons de notre succès auprès de très grandes entreprises françaises qui ont de nombreuses filiales à l'Etranger. Si Guillaume Poupard, DG de l'ANSSI, a parlé de notre sonde « GCap » lors de son discours d'ouverture aux dernières Assises de la Sécurité de Monaco, c'est parce que nous avons réussi à fabriquer une sonde suffisamment durcie pour résister aux « pentests » les plus exigeants tout en restant suffisamment agile pour analyser et détecter les intrusions. 200 sondes GCap sont déjà déployées dans le monde et nous estimons le marché potentiel des OIV à 2000 sondes ; sur les 7 appels d'offres qui ont eu lieu en 2018 sur ce sujet, Gatewatcher en a remporté 6... Aujourd'hui nous sommes 50 collaborateurs, dont 40 se consacrent à la recherche et au développement. Nous avons une forte croissance, avec l'objectif de réaliser 20M€ de chiffre d'affaires en 2020. Nous avons noué des partenariats de vente de nos produits avec de grands acteurs comme Orange, Atos, Sopra-Steria, etc.

➔ Quel avenir pour Gatewatcher ?

Notre cœur de métier est la sonde souveraine, mais de nouveaux produits arrivent. Exemple avec l'OS durci que nous avons monté, nous avons décidé d'en faire un produit à part entière : Gatewatcher Foundation. Il s'agit d'un OS serveur, qui est durci et en même temps flexible, adaptable selon le besoin. L'objectif est d'en faire un OS serveur adaptable aux besoins du client, en conciliant deux exigences : à la fois très sécurisé et très agile. Nous venons de déployer cet OS durci dans un très gros fonds d'investissement. Autre solution de développement : la GBox. Nous observons que sur le marché de la sécurité des SI, aujourd'hui, nous trouvons d'une part des produits de détection et d'autre part des produits d'analyse, souvent les clients ayant d'ailleurs tendance à confondre les deux. Or il faut arriver à distinguer le monde de la détection (trouver une intrusion avec les moyens adéquats) du monde de l'analyse (comprendre la menace que nous avons en face de nous), sachant que c'est une chaîne et qu'on ne peut pas faire l'analyse si rien n'a été détecter. C'est bien deux façons de voir les choses, même si elles sont complémentaires. Exemple, les personnes qui font de l'analyse ne sont pas les mêmes que celles qui font de la détection : les « hunters » qui cherchent les intrusions sont des investigateurs, alors que les analystes sont extrêmement techniques dans leur approche pour comprendre ce qui se passe avec un regard plus large.

➔ Chez Gatewatcher, on fait de la détection ou de l'analyse ?

Actuellement, nous faisons de la détection bien sûr pour identifier les comportements anormaux. Le but de la GBox, qui est une nouvelle « Appliance » d'analyse dynamique au travers de laquelle on va faire passer la menace, c'est d'émettre un rapport d'analyse complet pour comprendre cette menace. La GBox utilise plusieurs technologies de rupture, pour faire cette analyse dynamique : exemple, nous allons faire passer le fichier malicieux potentiel sur un Windows ad hoc (une bulle protégée), puis l'activer pour observer ce qui se passe, et ensuite faire un rapport. Nous procédons en ce moment à des tests pilotes de cette technologie et les résultats sont très prometteurs : nous observons ainsi tous les chemins d'exécution qui peuvent exister si le malware était dans un environnement différent, ce qui donne une arborescence d'actions qui enrichit un algorithme de machine learning. Exemple, avec Stuxnet qui était un virus dont le contexte d'exécution était déterminé par son écosystème applicatif (Iran). Avec la GBox, nous travaillons clairement sur des virus dont l'origine vient soit d'Etats, soit de mafias extrêmement puissantes. C'est une façon de faire de la contre-ingérence différemment, en remplaçant par une machine toute automatique ce que font aujourd'hui des centaines de personnes à la main et avec un certain coût chez certains opérateurs…Gatewatcher a donc un avenir passionnant !

Interview réalisée par Alain Establier

** Pour cette interview, Jacques de La Rivière était accompagné de Philippe Gillet, co-fondateur et directeur technique de Gatewatcher*

*** www.gatewatcher.com*