Choisir son fournisseur MSS

Alors que la transformation digitale des entreprises s'accélère, des mesures de protection parfois insuffisantes les exposent aux nouvelles menaces de la cybercriminalité.

En Europe, le coût de la cybercriminalité s'est accru de 35% au cours de la période 2014-2017 et pour 2017 son montant total est estimé entre 160 et 180 milliards de dollars[i]. En conséquence, la protection contre les menaces et la détection des incidents de sécurité sont des sujets prioritaires pour les directions IT.

Parallèlement, une étude d'ESG réalisée en 2018 sur les métiers de l'IT a mis en évidence les difficultés croissantes de recrutement de personnels compétents en cybersécurité. 53% des entreprises interrogées affirment être confrontées à ce problème de recrutement, soit une augmentation de 11% par rapport à 2015[ii].

Dans ce contexte, les Services Managés de Sécurité deviennent de facto le standard de l'arsenal défensif des entreprises.

Les Services Managés de Sécurité, ou « MSS », constituent la réponse appropriée aux enjeux de la sécurité numérique : surveillance et détection 24/7, analyse des incidents par des experts, accélération des opérations de réponse sur incident, mutualisation des retours d'expérience.

Nous vous proposons quelques thèmes de réflexions qui pourront vous aider à formuler vos critères de choix d'un fournisseur de services MSS :

- Maîtriser les coûts ;
- Partager les compétences ;
- Évaluer la maturité du fournisseur ;
- Personnaliser les services ;
- Choisir un fournisseur global ou local.

Maîtriser les coûts

Les principaux coûts d'un service MSS sont liés aux volumétries d'informations traitées et aux efforts d'adaptations consentis pas le fournisseur.

L'impact de l'accroissement des volumétries peut être clairement identifié et dans une certaine mesure, anticipé. Cependant, il est plus difficile d'apprécier les coûts associés à la mise en œuvre d'options complémentaires rendues nécessaires par les évolutions du business de l'entreprise et l'identification de nouvelles vulnérabilités. L'extension du périmètre des services nécessite, de la part du fournisseur, l'affectation de nouveaux moyens techniques et humains, et la mise en place de nouveaux processus adaptés aux exigences du client. Elle implique aussi des changements plus ou moins importants au sein de l'organisation du client.

C'est pourquoi, il nous semble essentiel de démarrer par une évaluation du Service MSS sur la base d'un périmètre restreint, représentatif des besoins de votre entreprise.

Durant quelques semaines d'expérimentation et de tests, challengez la capacité du fournisseur à adapter ses processus et ses services à votre organisation. Par ailleurs, au cours de cette période, vous pourrez préciser les métriques qui impacteront le coût du service.

Partager les compétences

La qualité des services managés de sécurité repose sur une bonne compréhension par l'opérateur de l'environnement du client, de ses habitudes de travail et de ses processus internes. Cela permet d'augmenter le taux de détection des incidents tout en réduisant les faux positifs, mais surtout de réduire significativement les délais de réponse aux incidents.

Ces améliorations résultent du partage efficace d'outils, de processus et de compétences entre le client et l'opérateur. Par exemple, il peut vous être utile d'accéder à des interfaces de surveillance et d'analyse pour faciliter les échanges entre vos équipes et celles du fournisseur. La collaboration entre l'opérateur et son client est un facteur clé pour améliorer les résultats et augmenter les bénéfices du service.

Privilégiez les acteurs aptes à répondre à vos besoins actuels et futurs : ils proposent des approches architecturales évolutives allant de la solution Cloud totalement managée, à diverses solutions hybrides.

Choisir son fournisseur MSS

Évaluer la maturité du fournisseur

Les outils mis en œuvre par les fournisseurs reposent sur des technologies qui ont considérablement évolué ces dernières années. Plus intelligentes et plus automatisées, elles permettent de faire face à des menaces ciblées de plus en plus complexes, et elles améliorent la proactivité.

Pour autant, assurer une supervision efficace et des réponses pertinentes nécessitent non seulement une parfaite gestion des outils mais aussi une connaissance approfondie de la cybersécurité et des modèles d'attaques. Sans cette connaissance, l'analyste en sécurité est démuni pour évaluer la gravité des alertes générées automatiquement par les outils.

Choisissez un acteur disposant d'une expérience validée par ses clients. Il a su mettre en œuvre les infrastructures et les processus qui lui permettent de maintenir la qualité de ses services tout en intégrant régulièrement de nouveaux clients, de toutes tailles.

Personnaliser les services

Vos besoins et vos contraintes sont uniques : le fournisseur de Services MSS doit apporter la réponse adaptée à votre entreprise.

Vous allez prendre un engagement à long terme avec votre fournisseur. Ce dernier doit être en mesure de répondre aujourd´hui à vos besoins sur votre périmètre technique (sites, logs, volumétrie, …) ainsi que dans les interactions avec vos équipes (helpdesk, partenaire tiers, outils IT).

Il devra en outre faire preuve de souplesse pour personnaliser le service et l'adapter rapidement aux changements que votre entreprise connaîtra.

Pour cela, validez de pouvoir échanger régulièrement avec les architectes en charge du service pour confronter vos besoins à leur roadmap.

Choisir son fournisseur MSS

Choisir un fournisseur global ou local ?

L'offre MSS est pléthorique. Des grands éditeurs de solutions de sécurité aux cabinets de conseils spécialistes en sécurité, des sociétés de service internationales aux intégrateurs de solutions locaux, comment s'y retrouver ?

Le fournisseur global, intervenant sur de multiples territoires présente l'avantage de disposer d'équipes importantes ; par sa taille il peut conserver un niveau technique adéquat mais sa souplesse et ses capacités d'adaptation restent limitées.

Quant au fournisseur local, il dispose d'une capacité de réaction et de personnalisation qu'aucun acteur global ne saurait lui contester. En revanche, il peut être confronté à des challenges opérationnels pour maintenir les niveaux d'expertise attendus.

Choisissez de préférence un acteur proposant une offre globalisée opérée à l'échelle européenne qui peut combiner cet avantage avec une capacité d'intervention locale.

Cette combinaison vous permettra de bénéficier du meilleur rapport coût/personnalisation et d'envisager sereinement un partenariat à long terme quelle que soit l'évolution de vos besoins.

Pedab est un opérateur européen de Services Managés de sécurité avec 25 ans d'expérience.

Pedab accompagne de multiples MSSP dans l'élaboration, la mise en œuvre et l'opération de leurs services de sécurité.

Le niveau d'expertise de son équipe conjuguée à l'utilisation de technologies de pointe assure un service reconnu pour les clients de toutes tailles.

Pedab se distingue sur le marché en proposant au travers de ses partenaires MSSP le meilleur compromis entre expertise, personnalisation de l'environnement client et capacité de réponse.

[i] Etude CSIS : https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf?kab1HywrewRzH17N9wuE24soo1IdhuHdutm_source=Pressutm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21utm_medium=emailutm_term=0_7623d157be-bb9303ae70-194093869

[ii] Etude ESG research: https://www.esg-global.com/blog/the-cybersecurity-skills-shortage-is-getting-worse