# Analyse de risques Ebios RM : la Fondation Cognacq-Jay utilise l'outil d'**ALL4TEC**

*La fondation Cognacq-Jay a utilisé l'outil d'analyse de risques de cybersécurité d'ALL4TEC à la clinique Saint-Jean-de-Dieu (Paris). Le bilan est positif : l'agilité de cet outil - le premier labellisé Ebios RM par l'Anssi - et son côté intuitif ont conquis les équipes.* ***Laurent Cosson,*** *PDG d'ALL4TEC,* ***Vincent Gerbier,*** *DSI de la clinique Saint-Jean-de-Dieu, et* ***Anne Auvity-Pontet,*** *responsable Transition et Innovation des SI à la fondation Cognacq-Jay, nous présentent ce projet.*

**DSIH :** ***Pourquoi avoir fait appel à ALL4TEC pour votre analyse de risques cyber ?***

**Anne Auvity-Pontet :** Dès 2019, nous nous sommes rendu compte que le monde de la santé devenait une cible et qu'il nous fallait une analyse de risques qui aille plus loin que ce que nous faisions, en prenant en compte le côté malveillance et pas uniquement les risques internes. Nous avons alors participé à une formation organisée par ALL4TEC. Leur produit était parfait : il correspondait à ce que nous recherchions et il était soutenu par l'Agence nationale de la sécurité des systèmes d'information, ce qui a été un critère majeur de choix.

***Quel est l'intérêt de la méthode Ebios Risk Manager (Ebios RM) ?***

**Laurent Cosson :** La méthodologie Ebios, qui existe depuis une vingtaine d'années, a été dépoussiérée en 2019 avec Ebios RM qui permet de passer d'une approche complètement tabulaire à une approche graphique. Cela permet de travailler en collaboration autour d'un écran, face à des visuels très intuitifs. Nous sommes très loin de l'informaticien seul dans son coin qui a parfois du mal à traiter les centaines de lignes et de colonnes de son tableau Excel !

**Vincent Gerbier :** L'approche tabulaire est une gageure en soi lors de la première itération ; à la deuxième, plus rien ne se synchronise. Avec Agile Risk Manager, nous pouvons en revanche repartir du projet, compléter une table et pas une autre, rescorer la gravité des impacts et les vraisemblances, etc. C'est un outil beaucoup plus agile. En tant que DSI de site, j'ai ainsi moins de mal à reprendre mon analyse pour la réitérer ponctuellement, à l'aune de nouvelles attaques.

***Une fois l'analyse effectuée, comment s'effectue le suivi du plan de maîtrise des risques ?***

**Laurent Cosson :** La méthode Ebios RM est divisée en cinq ateliers, dont le dernier est dédié au traitement du risque. Il aboutit à la définition de mesures de sécurité, recensées dans un plan d'amélioration continue de la sécurité (Pacs). L'outil permet de voir comment ces risques évoluent dans le temps. L'analyse des risques n'est pas une photo à un instant T, c'est un film.

**Vincent Gerbier :** Le côté graphique et dynamique de l'outil est très bien. Il permet de voir à trois, six ou huit mois si des risques sortent de la zone rouge pour passer en orange ou directement en vert. Ce côté intuitif facilite nos relations avec notre direction qualité et constitue un vrai levier de discussion. Quand j'ai montré l'outil à ma directrice qualité, elle m'a dit qu'elle voulait le même pour le suivi de ses plans d'actions ! Il est souvent difficile de parler de cybersécurité dans un établissement de santé, car elle est vue comme un truc d'informaticiens. Pour ceux qui auraient du mal à échanger avec leurs directions fonctionnelles respectives, cet outil est donc un réel atout en termes de communication.

**Laurent Cosson :** Ce côté « bottom-up », où l'on sensibilise les gens et où l'on remonte l'information vers les directions, est propre à la méthode Ebios RM. Mais notre outil apporte en plus des solutions pour bien organiser ces échanges.

***Quelles sont les prochaines étapes du projet ? Après le DPI de la clinique Saint-Jean-de-Dieu, allez-vous analyser les SI critiques des autres établissements de la Fondation ?***

**Anne Auvity-Pontet :** Notre feuille de route prévoit de continuer le déploiement sur les dossiers patients informatisés (DPI) des établissements de santé et sur les dossiers usagers (DUI) des autres établissements. Nous allons aussi mener une analyse de risques sur le système d'information du siège de la Fondation.

**Vincent Gerbier :** Et, au-delà des DPI, nous allons travailler sur d'autres systèmes d'information critiques essentiels : la stérilisation, la pharmacie, l'oncologie, etc.

**Laurent Cosson :** Un décret oblige les groupements hospitaliers de territoire, reconnus maintenant comme opérateurs de services essentiels (OSE), à procéder à des analyses de risques. Nous avons donc, avec notre partenaire dans la santé WELIOM, préparamétré des analyses de risques Ebios RM pour les dix systèmes d'information essentiels (SIE) concernés par cette réglementation. Ce gros travail d'instanciation, qui permet de gagner beaucoup de temps, est disponible auprès de la CAIH (Centrale d'achat de l'informatique hospitalière) qui a référencé notre outillage. ■