

Comment deux services de police britanniques ont considérablement amélioré leur efficacité et leur niveau de contrôle en centralisant la gestion numérique de leurs preuves

ÉTUDE DE CAS

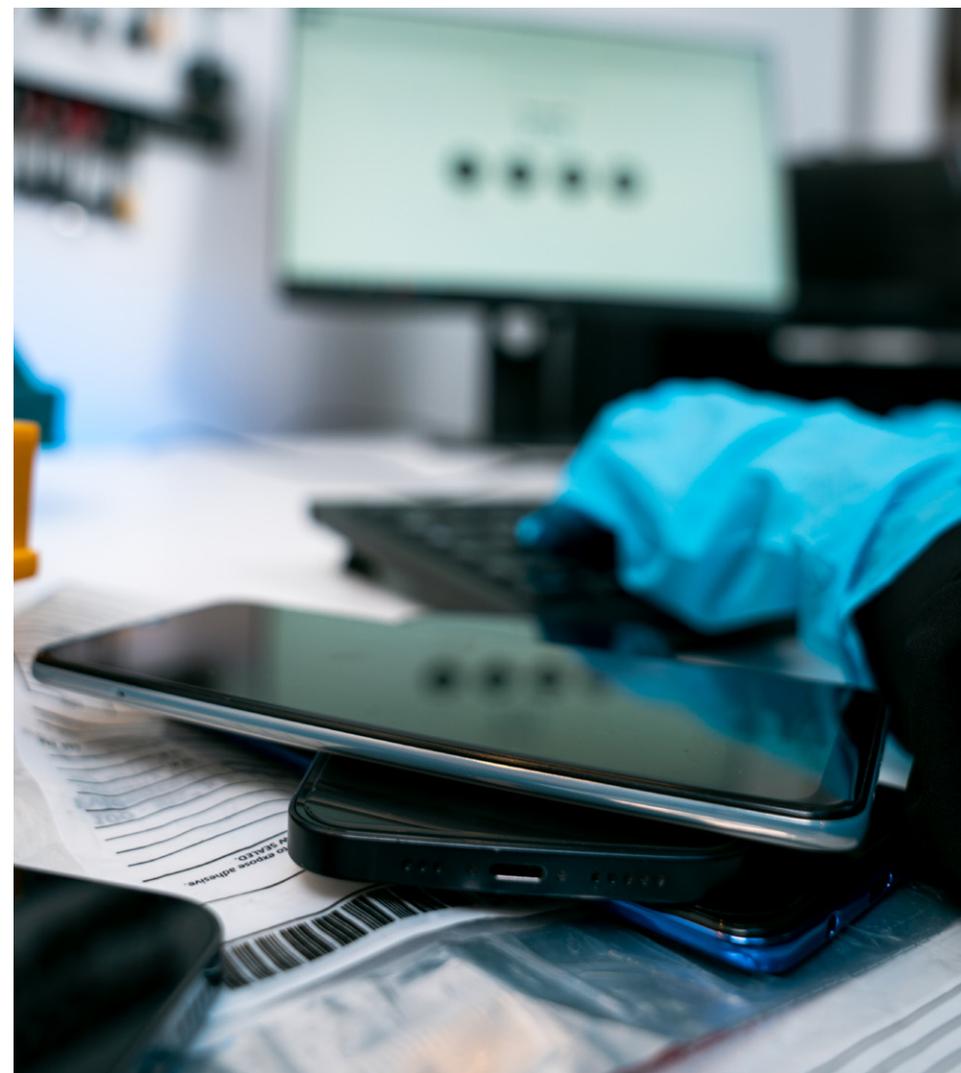
IL Y A QUELQUES ANNÉES, deux services de police britanniques ont fusionné leurs équipes de criminalistique numérique afin de faire des économies et de gagner en efficacité. L'unité nouvellement créée comptait environ 200 agents formés et répartis sur plusieurs sites distants. Elle utilisait le logiciel XRY pour enquêter sur toutes les affaires où le numérique entraînait en jeu.

Mais l'Unité de criminalistique numérique se heurtait à un certain nombre de difficultés :

- Des retards étaient constatés au niveau de l'extraction des données des dispositifs mobiles et de leur analyse.
- Les ordinateurs utilisés par la police scientifique pour le stockage des dossiers d'extraction mobile présentaient un espace insuffisant. En conséquence, les agents étaient souvent réticents à télécharger les données de téléphone nécessitant un traitement.
- Les ordinateurs n'étant pas reliés en réseau, le logiciel XRY était rarement actualisé. Les mises à jour logicielles envoyées sur des disques étaient installées de manière aléatoire.
- Dès lors, il était difficile d'assurer cohérence et qualité de travail sur l'ensemble des sites.
- Les utilisateurs modifiaient régulièrement les profils de téléchargement en dépit des consignes du responsable de l'unité.
- Les utilisateurs individuels changeaient de mot de passe, rendant compliquée la récupération des identifiants de connexion.
- Les dossiers extraits étaient gravés sur des DVD et devaient être transportés physiquement là où les données étaient requises, ce qui

nécessitait jusqu'à 3,5 heures de route et était « source de problèmes et d'inquiétudes constantes ».

- L'analyste en criminalistique numérique responsable de l'Unité a résumé ainsi les défis rencontrés : « Nous n'avions aucune idée de qui accédait aux machines, pour quelle raison, à quelle fréquence, de quelle quantité de données était téléchargée, d'où se trouvaient les données et de qui y avait accès ».



« Lorsque j'ai découvert le MSAB Kiosk et ses capacités réseau, j'en suis tombé amoureux, a déclaré l'analyste en criminalistique numérique responsable de l'Unité. Mais il m'a fallu des années pour obtenir son approbation. »

Au Royaume-Uni, tous les laboratoires de criminalistique numérique de la police sont tenus de respecter le système de gestion de la qualité selon la norme ISO 17025 afin de garantir la cohérence et la qualité de leur travail.

Changer le statu quo : adopter un nouveau tournant

« J'ai fait valoir le fait que la norme ISO 17025 serait mise en œuvre en amont de la criminalistique mobile. Dès lors, si nous voulions disposer des mêmes capacités pour les cas où nous avons du personnel sur le terrain, afin d'obtenir des résultats exploitables de manière cohérente, nous avons de toute façon besoin d'une infrastructure en réseau à l'avenir. Pourquoi ne pas l'implémenter dès maintenant ? Cela nous aiderait à nous conformer à la norme ISO 17025. »

« J'ai également insisté sur le fait que la mise en place d'un environnement en réseau permettrait le téléchargement immédiat des données plutôt que d'attendre de les recevoir via un disque de stockage. Le déplacement et la mise à jour des unités prenaient deux jours, un temps qui aurait été mieux mis à profit en aidant à l'enquête. »

« Nous avons plus de 30 postes de police où des personnes s'efforcent de faire leur travail au quotidien. En conséquence, lors du téléchargement des données téléphoniques du suspect, il n'est pas rare que l'enquêteur qui attend de pouvoir analyser les données se trouve dans un autre lieu. »

L'adoption des mesures relatives au RGPD, au règlement général sur la protection des données, qui visent à préserver la confidentialité et prévoit

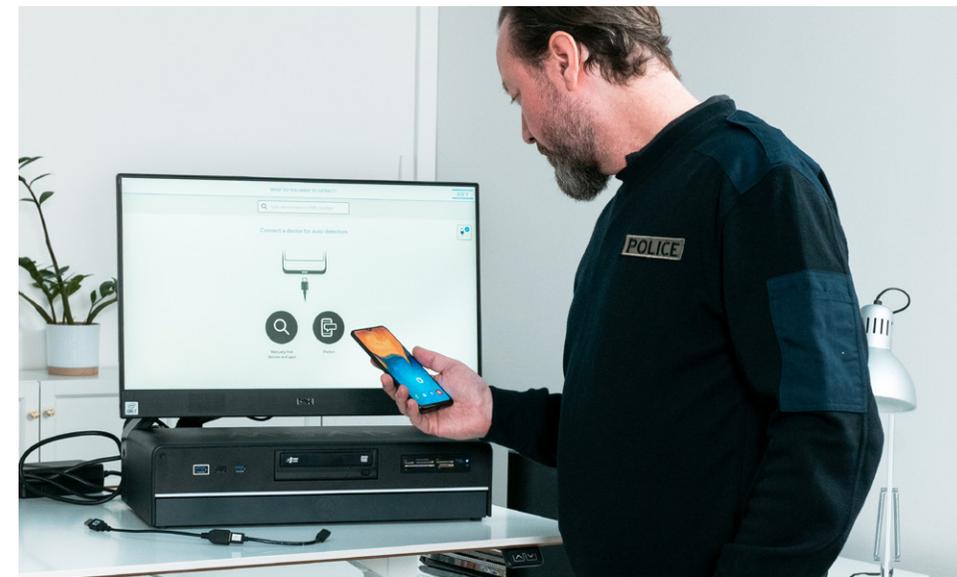
une amende élevée en cas de violation, était un autre facteur en faveur d'un changement de statu quo.

« Mon argument portait sur le risque attaché à la perte d'un disque contenant les données personnelles d'un individu, et l'amende d'un million de livres en résultant. »

Faire évoluer les choses : la phase de mise en œuvre

« Tout a été mis en œuvre super rapidement une fois toutes les approbations obtenues. Il nous a fallu huit semaines entre l'arrivée des Kiosks et leur mise en service. » « Nous n'avons rencontré aucune difficulté. Il nous a juste fallu appuyer sur un bouton. »

« MSAB a été formidable et nous a apporté toute son assistance. Nous avons eu l'équipe au téléphone plusieurs fois. À différentes reprises, nous avons demandé à ses membres de se rendre sur place pour aider à l'installation et aux essais. Ils sont intervenus sur le site bien avant la mise en service. MSAB nous a offert le meilleur des soutiens. Depuis lors, tout va très bien. »



Depuis que les deux services de police ont installé le logiciel XEC Director et lié tous leurs Kiosks, les fichiers d'extraction sont désormais envoyés vers un serveur central. Les fichiers ne sont plus gravés sur des DVD et chaque utilisateur dispose de son propre dossier. Il n'est plus question de manque d'espace de stockage.

« La solution de MSAB a eu un impact positif sur nos forces combinées.

- Les données sont accessibles entre les deux services presque instantanément. Ainsi, si un meurtre a lieu dans un comté, mais que les enquêteurs se trouvent dans un autre, il n'est pas nécessaire d'attendre l'arrivée des DVD et leur copie. Nous avons maintenant accès aux données quasiment en temps réel.
- Il est désormais possible de gérer toutes les mises à jour du logiciel XRY grâce à XEC Director. Cela signifie moins de perte de temps en conduite et des économies importantes. Jusqu'à présent, les Kiosk ont été exceptionnellement stables, et leur fonction de détection automatique s'est révélée remarquable.
- Les utilisateurs ne touchent plus à XRY depuis l'arrivée des Kiosks. De plus, comme le flux de travail est là pour les aider pas à pas, ils n'hésitent plus à utiliser le logiciel. Ils adorent sa rapidité d'exécution. Ils n'ont plus à craindre que le système se bloque ou manque d'espace.
- Les utilisateurs se sentent mieux armés grâce au contrôle qu'ils peuvent désormais exercer. Les mises à jour logicielles peuvent être facilement diffusées. En cas de problème, les responsables sont en mesure d'aider les utilisateurs même s'ils ne sont pas sur place. En tant que responsable, je peux voir la quantité de données que nous produisons. La fonction de rapport est très utile pour moi. Et comme

nous sommes en mesure d'établir des rapports clairs et concis à l'intention de la direction, nous allons poursuivre l'acquisition de nouveaux Kiosks.

— Pour résumer. Je dispose désormais d'un environnement configuré et contrôlé de manière centralisée, et toutes les données sont sauvegardées dans une solution de stockage centrale. Nos utilisateurs sont en mesure d'utiliser les dernières versions de XRY et du logiciel de données forensiques mobiles XAMN. Autre atout majeur : la direction a perçu tous les avantages de cette solution. »

➤ « Le passage au Kiosk de MSAB et à un système en réseau a été la meilleure décision que nous ayons jamais prise. Aujourd'hui, par exemple, nous sommes mieux à même d'aider les victimes de violence domestique courant un risque élevé.

Auparavant, faire appel au laboratoire retardait le processus d'au moins un mois. L'utilisation de Kiosk nous permet désormais de confronter l'agresseur aux preuves extraites lors de l'entretien. Une accusation peut être portée au cours des huit premières heures. »

– Analyste en criminalistique numérique
responsable de l'Unité