

ÉTUDE DE CAS – BUREAU DU SHÉRIF DU COMTÉ DE KERR

MAGNET ATLAS™

Comment le bureau d'un shérif texan raccourcit le temps passé sur les enquêtes numériques



Nous ne perdons rien de vue et nous obtenons un délai d'exécution très rapide pour nos appareils. ATLAS contribue à maintenir ce flux. »

— Lucas Flores, enquêteur en criminalistique numérique, bureau du shérif du comté de Kerr

Le défi

Dès que la nouvelle s'est répandue, les demandes ont afflué.

Lucas Flores gère chaque jour ce qu'il traitait auparavant pendant un mois entier.

En tant qu'unique enquêteur à temps plein pour le bureau du shérif du comté de Kerr dans le centre du Texas, Flores a vu les demandes de preuves numériques passer d'un ou deux appareils par mois à 30 appareils au cours de la même période.

La croissance exponentielle observée en quelques années est due aux progrès technologiques et à l'augmentation des capacités.

« Chaque crime commis a désormais une empreinte numérique », explique M. Flores.

Son laboratoire à service complet répond aux intrusions et aux appels de rançongiciels, bien que d'autres infractions pénales, dont les affaires de stupéfiants qui représentent la moitié de la charge de travail, génèrent également des preuves numériques par le biais de messages textes, d'itinéraires cartographiés, d'enregistrements de caméras de sonnettes et bien d'autres choses encore. Un seul cas d'exploitation d'enfant peut donner lieu au traitement d'une douzaine d'appareils.



Le bureau du shérif du comté de Kerr veille à l'application de toutes les lois et ordonnances, protège la vie et les biens, préserve la paix et s'efforce de prévenir la criminalité et le désordre.

Situé à Kerrville, Texas

Au service de plus de 60 000 citoyens

ENQUÊTES

- La criminalistique numérique, l'enquête électronique et la récupération de données
- Sécurité des données et respect de la vie privée
- Tests de pénétration et services de sécurité gérés

RÉSULTATS

- Réduction du nombre d'heures de réception et de traitement
- Élimination des appels pour vérifier l'état d'avancement du dossier
- Pilote le déroulement des affaires au sein d'une équipe dispersée



Étant seul, Flores est de plus en plus occupé. Il a ensuite obtenu la certification du National Computer Forensics Institute (NCFI) et la nouvelle s'est répandue. « La formation et l'équipement n'ont fait qu'alourdir ma charge de travail, car j'avais plus de capacités », explique-t-il.

La paperasse et les feuilles de calcul ne pouvaient pas suivre.

À ses débuts, Flores coordonnait les preuves numériques à l'aide de formulaires papier empilés dans un classeur.

Le siège du comté étant situé à Kerrville, la plus grande ville située à 800 kilomètres entre San Antonio et El Paso, les agents pouvaient faire des heures de route pour déposer un téléphone et remplir une demande. Flores a suivi les efforts manuellement, en feuilletant les pages chaque fois qu'un demandeur appelait pour vérifier l'état d'avancement.



J'ai rapidement réalisé à quel point le suivi sur papier des enquêtes sur les preuves numériques était ingérable.

J'avais besoin de quelque chose de plus convivial. »

À cette fin, Flores a commencé à suivre les dispositifs à l'aide de feuilles de calcul avec des liens hypertextes vers des images scannées des formulaires de demande et d'autorisation de recherche.

« Les feuilles de calcul étaient plus jolies, mais elles étaient tout aussi fastidieuses, si ce n'est plus. Cela nous a pris beaucoup de temps. »

L'utilité de Magnet ATLAS

Une plaque tournante pour accélérer le traitement des dossiers

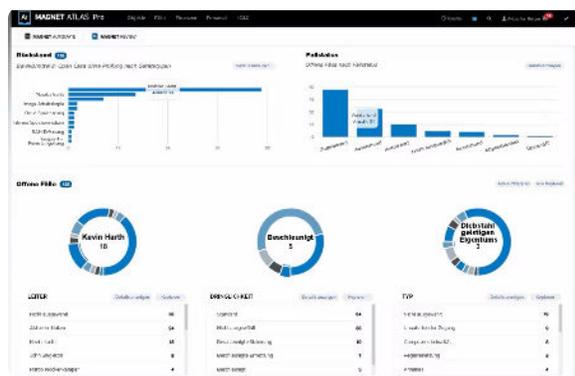
Bien que Flores ait obtenu une aide à temps partiel, il a reconnu la nécessité de relever les défis numériques grâce à une solution numérique moderne.

« Le nombre de preuves disponibles est énorme. Pour que nous puissions nous en occuper efficacement, il faut d'abord gérer le laboratoire. »

Renonçant au papier et aux feuilles de calcul, Flores s'est tourné vers Magnet ATLAS™ pour mener des enquêtes numériques. Le bureau du shérif de Kerr utilise également Magnet AXIOM™ ainsi que d'autres outils de découverte et d'analyse.

Flores décrit l'impact du logiciel de gestion de laboratoire collaboratif ATLAS comme « un véritable changement », qui a permis de gagner des jours entiers sur la rotation des appareils et le flux de travail par rapport aux méthodes antérieures. Son laboratoire a acquis la réputation d'être l'endroit où il fallait aller pour faire avancer les choses.

« Nous gardons la maîtrise des choses et nous obtenons un délai d'exécution très rapide pour nos appareils. ATLAS contribue à maintenir ce flux. »



La centralisation permet d'accélérer les délais

Grâce à ATLAS, les agents et les enquêteurs peuvent soumettre eux-mêmes des demandes et des documents d'autorisation de recherche, même à distance, ce qui leur permet, ainsi qu'à Flores, de gagner du temps. « La possibilité de confier à d'autres la responsabilité d'une partie des données me permet de gagner des heures chaque jour », a-t-il déclaré. Lorsque Flores a terminé l'enregistrement, il lui suffit de télécharger une photo de l'appareil et d'imprimer les étiquettes.

« ATLAS a été d'une aide précieuse dans l'organisation du laboratoire et l'amélioration de l'efficacité », explique Flores. « Chaque prise en charge ne prend que cinq minutes au lieu d'une heure, ce qui me permet de passer à l'examen plus rapidement. »

Ensuite, toutes les données relatives aux dossiers sont gérées, suivies et disponibles via ATLAS. Lorsqu'un dispositif est prêt, Flores assure un gain de temps en permettant aux parties prenantes de se connecter et d'accéder directement aux résultats.



ATLAS fait tout ce dont j'ai besoin.

Je dispose désormais d'une chaîne de contrôle, de photographies, d'un exposé des faits... tout est réuni en un seul endroit et c'est fantastique. »

En outre, ATLAS peut être adapté aux besoins du bureau du shérif du comté de Kerr en matière de rapports. « Ce n'est pas un logiciel conçu pour une utilisation limitée », précise Flores. « Les possibilités de personnalisation me permettent de collecter et de communiquer les données spécifiques aux autorités judiciaires dont je relève. »

La collaboration améliore la productivité

Qu'il se trouve dans le même bâtiment ou à 200 km de là, tout membre de l'équipe disposant d'un accès approuvé en fonction de son rôle peut contribuer à une enquête active. Ils peuvent également obtenir des rapports en temps réel et des rapports historiques en libre-service, ce qui évite à Flores de devoir se consacrer à d'autres tâches non essentielles.

« Je ne reçois plus d'appels me disant : J'ai appelé il y a 45 minutes. Est-ce que c'est fini maintenant ? » explique Flores. « Au lieu de cela, je leur dis : On s'en occupe. Vous recevrez des e-mails au fur et à mesure de l'avancement des travaux et vous serez informés à la fin de l'examen lorsque nous cliquerons sur le bouton finaliser ».

Si un membre de l'équipe contacte encore Flores pour localiser un appareil, il recherche simplement le numéro CSE, et trouve parfois même que le demandeur a signé pour l'appareil la semaine précédente.

L'art de clore l'affaire

Le gain de temps est un résultat appréciable. En veillant à ce que les heures de travail de son enquêteur principal soient consacrées aux examens plutôt qu'aux tâches administratives, le bureau du shérif du comté de Kerr poursuit sa mission d'application de la loi.

Les délais plus courts et les efforts efficaces rendus possibles par la gestion du laboratoire ATLAS soutiennent l'ensemble de l'équipe dans l'élaboration d'un dossier solide.

« La criminalistique numérique est un travail acharné et minutieux », note Flores. « C'est un soulagement de trouver un système efficace pour gérer les preuves numériques critiques à l'appui de la justice. »

Flores a indiqué que la mise en œuvre d'ATLAS par son service avait été un succès en termes de retour sur investissement. En fait, il se fait le champion de la solution auprès d'autres organisations lorsqu'il en a l'occasion.



« Je frémis à l'idée de devoir revenir un jour aux feuilles de calcul », conclut-il.

« Pour pouvoir les aider, je dis à tout le monde qu'ils ont besoin de Magnet ATLAS. »

Pour en savoir plus sur Magnet ATLAS et découvrir son fonctionnement, veuillez consulter le site magnetforensics.com/magnet-atlas.

© 2022 Magnet Forensics Inc. Tous droits réservés. Magnet Forensics® et les marques commerciales associées sont la propriété de Magnet Forensics Inc. et de ses filiales et sont utilisées dans des pays du monde entier.

