FALLSTUDIE – SHERIFF-BÜRO VON KERR COUNTY

MAGNET ATLAS™

Wie ein texanisches Sheriff-Büro seine digitalen Ermittlungen um Tage beschleunigt

> Wir bleiben direkt dran und haben bei unseren Geräten eine sehr schnelle Bearbeitungszeit. ATLAS trägt entscheidend dazu bei, dass das so bleibt."
>
> — **Lucas Flores, Ermittler für digitale Forensik, Sheriff-Büros von Kerr County**

Die Herausforderung

Als sich das herumgesprochen hatte, strömten die Anfragen nur so herein.

Inzwischen bearbeitet Lucas Flores jeden Tag das, was er früher in einem ganzen Monat bearbeitete.

Flores, der einzige Vollzeit-Ermittler für digitale Forensik im Sheriff-Büro von Kerr County in Zentraltexas erlebte, wie die Anträge für Durchsuchungen nach digitalem Beweismaterial von ein oder zwei Geräten pro Monat auf bis zu 30 Geräte für denselben Zeitraum gestiegen sind.

Das exponentielle Wachstum innerhalb weniger Jahre ist auf den technologischen Fortschritt und die erweiterten Möglichkeiten zurückzuführen.

„Heutzutage hinterlässt jedes Verbrechen irgendeine Art digitaler Spuren", erklärt Flores.

Sein umfassend ausgestattetes Labor bearbeitet Zugriffsversuche und Ransomware-Angriffe sowie sonstige Straftaten – einschließlich Rauschgiftdelikten, die die Hälfte des Arbeitsvolumens ausmachen – und generiert digitale Beweise in Form von Textnachrichten, Routenplänen, Aufnahmen von Türklingelkameras und mehr. Ein einziger Fall von Kinderausbeutung kann die Bearbeitung von einem Dutzend Geräten umfassen.

Das Sheriff-Büro von Kerr County ist für die Durchsetzung aller Gesetze und Verordnungen, den Schutz von Leben und Eigentum, die Wahrung des Friedens und die Verhinderung von Verbrechen und Unruhen zuständig.

Ansässig in Kerrville, Texas

Für mehr als 60.000 Bürger zuständig

ERMITTLUNGEN

- Digitale Forensik, eDiscovery, & Datenwiederherstellung
- Datensicherheit und Einhaltung des Datenschutzes
- Penetrationstests und Managed Security Services

ERGEBNISSE

- Spart Stunden bei der Erfassung und Bearbeitung
- Eliminiert Anrufe zu Statusfragen
- Fördert den Arbeitsablauf unter verstreut sitzenden Teammitgliedern

Als einziger Ermittler hatte Flores immer mehr zu tun. Er erhielt die Zertifizierung vom National Computer Forensics Institute (NCFI) und das sprach sich herum. Die Schulung und die Ausrüstung erhöhten meine Arbeitslast weiter, weil ich mehr Möglichkeiten hatte", sagt er.

Papierkram und Tabellenkalkulationen reichten nicht mehr aus.

Zu Beginn seiner Tätigkeit koordinierte Flores digitale Beweise über Papierformulare, die er in einem Ordner aufbewahrte.

Da sich der Sitz des Bezirks in Kerrville befindet, der nächstgrößeren Stadt im Umkreis von 500 Meilen zwischen San Antonio und El Paso, waren die Beamten oft Stunden unterwegs, um ein Telefon abzugeben und einen Antrag auszufüllen. Flores erfasste die Arbeit manuell und durchsuchte jedes Mal die Seiten, wenn ein Antragsteller anrief, um sich über den Status zu informieren.

> Mir wurde schnell klar, dass die Nachverfolgung digitaler Beweismittel auf Papier untragbar war. Ich brauchte etwas Benutzerfreundlicheres."

Aus diesem Grund begann Flores, die Geräte in Tabellendokumenten mit Hyperlinks zu gescannten Bildern von Antragsformularen und Formularen für Durchsuchungsbefehle zu erfassen.

„Tabellendokumente sahen zwar schöner aus, aber sie waren genauso aufwendig, wenn nicht noch aufwendiger." Es kostete viel Zeit, sich damit zu beschäftigen."

Wie Magnet ATLAS hilft

Eine Drehscheibe für eine schnellere Fallbearbeitung

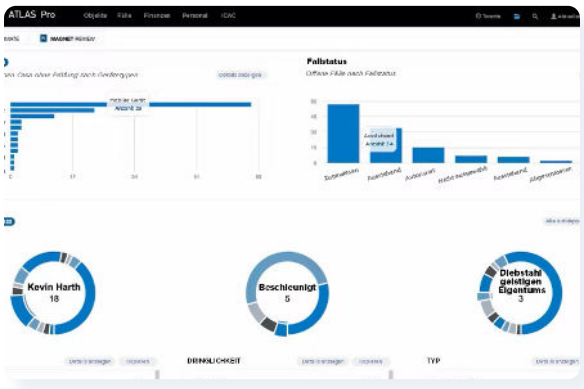
Obwohl Flores Teilzeitunterstützung bekam , erkannte er die Notwendigkeit, den digitalen Herausforderungen mit einer modernen digitalen Lösung gerecht zu werden.

„Die Menge an Beweisen ist enorm. Damit wir sie effektiv bearbeiten können, müssen wir zunächst das Labor organisieren."

Flores schaffte Papier und Tabellenkalkulationen ab und entschied sich für Magnet ATLAS™, um digitale Ermittlungen durchzuführen. Das Sheriff-Büros von Kerr County verwendet Magnet AXIOM™ auch zusammen mit anderen Ermittlungs- und Analysetools.

Flores beschreibt die Vorteile der ATLAS-Software für das kollaborative Labormanagement als „einen absoluten Wendepunkt"Sie brachte im Vergleich zu früheren Methoden eine Zeitersparnis von mehreren Tagen bei der Bearbeitung von Geräten und bei den Arbeitsabläufen. Sein Labor hat sich den Ruf erworben, die richtige Anlaufstelle zu sein, um Sachen auf den Grund zu gehen.

Wir bleiben direkt dran und haben bei unseren Geräten eine sehr schnelle Bearbeitungszeit. ATLAS trägt entscheidend dazu bei, dass das so bleibt."



Die Zentralisierung sorgt für eine schnellere Bearbeitung

Mit ATLAS können Beamte und Ermittler selbst sogar mittels Fernübermittlung Anträge und Dokumente für Durchsuchungsbefehle einreichen, was ihnen und Flores Zeit spart. „Die Möglichkeit, dass andere für einen Teil der Eingaben verantwortlich sind, spart mir jeden Tag Stunden", sagte er. Wenn Flores die Erfassung abgeschlossen hat, lädt er einfach ein Foto des Geräts hoch und druckt Etiketten aus.

„ATLAS ist eine große Hilfe bei der Organisation des Labors und der Steigerung der Effizienz", erzählt Flores. „Jede Erfassung eines Geräts dauert nur noch fünf Minuten statt einer Stunde, was bedeutet, dass ich schneller mit der Untersuchung beginnen kann."

Anschließend Anschließend werden alle Falldaten mit ATLAS verwaltet, sind dort nachverfolgbar und zugänglich. Flores spart nach Abschuss der Untersuchung eines Geräts durch die Vergabe von direkten Zugriffsrechten auf die Ergebnisse an die Beteiligten Zeit.

> ATLAS erledigt alles, was ich brauche. Jetzt habe ich eine Beweiskette, Fotos, den Bericht ... alles an einem Ort und das ist fantastisch."

Zudem lässt sich ATLAS an die Bedürfnisse hinsichtlich der Berichtserstellung des Sheriff-Büros von Kerr County anpassen. „Es ist keine Software, die man so wie sie ist, akzeptieren muss", sagt Flores. „Die Anpassungsmöglichkeiten erlauben es mir, die Daten zu erfassen und zu melden, die für meinen Zuständigkeitsbereich relevant sind."

Zusammenarbeit steigert die Produktivität

Ob im selben Gebäude oder 200 Meilen entfernt, jedes Teammitglied mit genehmigtem aufgabenbasiertem Zugriff kann zu einer aktiven Ermittlung beitragen. Sie können zudem selbstständig Echtzeit- und historische Berichte abrufen, sodass Flores sich auf fallkritische Aufgaben konzentrieren kann.

„Ich bekomme keine Anrufe mehr, in denen es heißt: Ich habe das Telefon vor 45 Minuten abgegeben. 'Sind Sie schon fertig?' ", sagt Flores. „Stattdessen sage ich ihnen: Wir kümmern uns darum. Sie werden per E-Mails über die Fortschritte informiert. Sobald die Untersuchung abgeschlossen ist und wir „abschließen" anklicken, werden Sie benachrichtigt."

Wenn ein Teammitglied Flores dennoch kontaktiert, um ein Gerät ausfindig zu machen, sucht er einfach nach der CSE-Nummer und findet manchmal sogar den Antragsteller, der in der Vorwoche dafür unterschrieben hatte.

Unterstützung für den Abschluss des Falles

Zeitersparnis ist ein willkommenes Ergebnis. Die Mission des Sheriff-Büros von Kerr County, die Gesetze durchzusetzen, wird durch die Gewährleistung unterstützt, dass leitende Ermittler ihre wertvolle Zeit nicht mit intensiver Fleißarbeit verbringen müssen, sondern sich auf die Ermittlungen konzentrieren können.

Die durch das ATLAS-Labormanagement ermöglichte schnellere und effektivere Bearbeitung unterstützt ein ganzes Team beim Auffinden und Sichern von Beweisen.

„Digitale Forensik ist eine unerbittliche, detaillierte Arbeit", erklärt Flores. „Es ist eine Erleichterung, ein effizientes System für die Verarbeitung wichtiger digitaler Beweise zur Unterstützung der Justiz zu finden."

Flores zufolge hat sich die Implementierung von ATLAS in seiner Abteilung bezahlt gemacht. Er setzt sich sogar bei jeder sich bietenden Gelegenheit für diese Lösung bei anderen Organisationen ein.

> „Mich schaudert es bei dem Gedanken, jemals wieder zu Tabellendokumenten zurückkehren zu müssen", sagt er abschließend.
> „Um ihnen zu helfen, sage ich allen, dass sie Magnet ATLAS brauchen."

Erfahren Sie mehr über Magnet ATLAS und sehen Sie es im Einsatz unter magnetforensics.com/magnet-atlas.

MAGNET FORENSICS®