

Lösungen für Entitäts- und Beziehungsanalysen für die öffentliche Sicherheit

Sammeln Sie Daten aus unterschiedlichen Datenquellen als Grundlage für effiziente Untersuchungen, genaue Informationen und ein besseres Situationsbewusstsein



Im heutigen Zeitalter der uneingeschränkten persönlichen Mobilität stehen die Strafverfolgungsbehörden vor einer fast unlösbaren Herausforderung im Zusammenhang mit Daten. Wie können Ermittler angesichts riesiger Mengen an Daten, relevante Informationen über Personen, Objekte, Orte und Ereignisse sammeln und schnell miteinander verknüpfen?

Auch wenn die Beamten versuchen, ihre Daten zu strukturieren, nimmt die Arbeitsbelastung immer weiter zu. Ungelöste Fälle, die Komplexität der organisierten Kriminalität, die Verschleierung von kriminellen Identitäten und Beziehungen und die unglaublich hohe Zahl von Datenquellen mit möglichen Informationen über Straftaten und Kriminelle kann die Beamten überfordern. Der Umfang dieser Aktivitäten und Arbeitsvorgänge schränkt die Fähigkeit der Ermittler ein, schnell die Verbindungen zu erkennen, die den Abschluss von Untersuchungen ermöglichen.

Häufig bleiben Fälle nicht aus Mangel an Daten ungelöst, sondern aufgrund der Schwierigkeit, Erkenntnisse aus bereits vorliegenden Daten zu gewinnen. Die Lösung eines Falls anhand von vieler Daten ist oft genau so schwierig wie der Versuch, einen Fall mit zu wenig Informationen lösen zu wollen. Die Beamten müssen nicht nur bestimmen, wie die Daten zusammenpassen, sondern auch erkennen, welche die relevantesten sind. Wenn Ermittler diese Erkenntnisse zu einem früheren Zeitpunkt gewinnen könnten, müssten sie weniger Zeit für die Suche nach Informationen aufwenden und könnten sich stärker darauf konzentrieren, wofür sie ausgebildet sind: Beweise zu analysieren und Straftaten aufzuklären. Technologische Fortschritte, z. B. Fingerabdruck- und DNA-Tests, die zu einer überzeugenden Daten- und Analysestrategie führen, verringern den manuellen Aufwand im Zusammenhang mit der Suche nach Informationen in unterschiedlichen Datenquellen, mit denen sich wiederum Informationen in Erkenntnisse umwandeln lassen.

Ganzheitliche Analysen für schnelle Ergebnisse

Im gesamten öffentlichen Sektor steigt der finanzielle Druck, mit weniger Mitteln mehr Aufgaben zu erledigen. Der Bereich Strafverfolgung bildet da keine Ausnahme. Die Bürger erwarten allerdings Ergebnisse. Wie kann die richtige Daten- und Analysestrategie Sicherheitsbehörden dabei helfen, bessere Einblicke zu erhalten? Das Hauptziel besteht natürlich darin, Verdächtige schnell zu identifizieren und einen Fall auf der Grundlage von Beweisen anzulegen. Das Zusammenführen der Beweise ist für das Anlegen eines Falls entscheidend – unabhängig davon, in welchem Format sie vorliegen. So kann analysiert werden, inwieweit sie mit Verdächtigen in Verbindung stehen, mit welchen Personen sie Kontakt haben, welche Orte sie häufig besuchen und welche Gegenstände damit verknüpft sind.

Kurz gesagt, kann eine Analysestrategie auf der Grundlage ganzheitlicher Betrachtungsweise zur Verbesserung der Verfahren zur Identifizierung und Ermittlung von Straftaten beitragen. Diese Analysen beinhalten die minutengenaue Identifizierung bekannter Straftäter, gesuchter Personen, Opfer und Zeugen sowie deren Beziehung untereinander. Dies gilt auch dann, wenn die Informationen, durch die diese Personen miteinander verbunden sind, über mehrere Datenquellen verteilt sind. Die Analysen können auch modernste Methoden zur Darstellung dieser nicht offensichtlichen Beziehungen beinhalten und Ermittler, Analysten und Außendienstmitarbeiter proaktiv benachrichtigen, sobald neue Informationen zur Verfügung stehen.

Strategische Zusammenarbeit mit Strafverfolgungs- und Sicherheitsbehörden

Die IBM InfoSphere-Plattform umfasst eine Reihe von Produkten, die Strafverfolgungsbehörden bei der Entwicklung der immer wichtiger werdenden Strategien bei Datenanalysen helfen. IBM InfoSphere Identity Insight wurde entwickelt, um Echtzeitfunktionen zur Identifizierung von Verbindungen zwischen Einheiten zu liefern. Dabei wird auf Daten aus praktisch jeder Quelle zurückgegriffen. Im Gegensatz zu anderen Ansätzen zur Gewinnung von Erkenntnissen, bei denen Datenquellen wiederholt manuell oder übergreifend durchsucht werden, um die sprichwörtliche „Nadel im Heuhaufen“ zu finden, findet InfoSphere Identity Insight die nicht offensichtlichen Zusammenhänge, die nur durch eine gründliche Analyse der aufgelösten Entitätsinformationen identifiziert werden können.

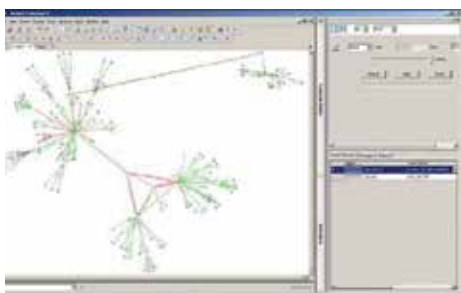


Abbildung 1: Identifizierung nicht offensichtlicher Beziehungen durch grafische Analysen mit InfoSphere Identity Insight und dem i2 Analyst's Notebook.

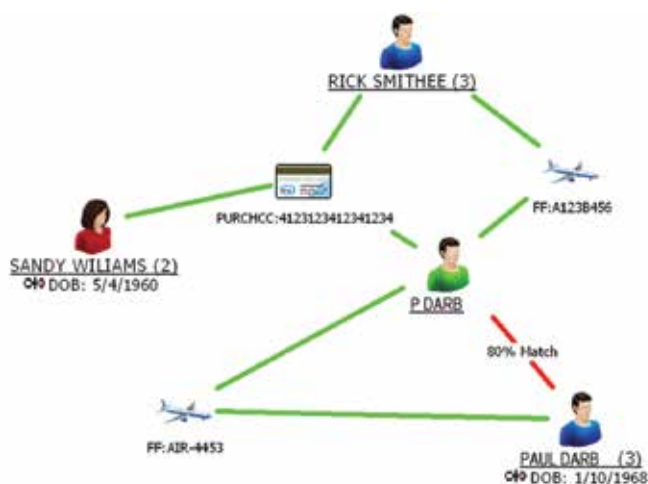
Die Software kann selbst scheinbar unauffällige Beziehungen zwischen Opfern, gesuchten Personen und Zeugen analysieren. Da hierbei nicht offensichtliche Zusammenhänge gefunden werden, die nur durch eine ganzheitliche Entitätsauflösung über verschiedene Datenquellen hinweg möglich ist (siehe Abbildung 1), liefert die Analyse Erkenntnisse, die durch menschliche Interpretation und manuelles Abgleichen nur schwer zu erreichen sind. Diese Erkenntnisse sind bei der Kombination von Datenquellen dennoch nur schwer zu erkennen, da die einzelnen Quellen aufgrund uneinheitlicher Dateneingaben, einer Verschlechterung der Daten und absichtlicher Verschleierung oft nicht vertrauenswürdig sind.

InfoSphere Identity Insight nutzt die vom US Department of Homeland Security nach dem Safety Act genehmigte IBM Global Name Recognition, um komplexe Namensabweichungen zu analysieren, die sich aus unterschiedlichen kulturellen und geografischen Herkünften ergeben. Diese Analyse hilft Ermittlern, die mögliche unterschiedliche Schreibweisen und nicht intuitive Verbindungen zwischen Vornamen und Spitznamen untersuchen müssen (siehe Abbildung 2).

Da InfoSphere Identity Insight die Analysen in Echtzeit durchführt, auf Daten aus verschiedenen Quellen zugreift und Benachrichtigungen sendet, sobald neue Informationen von einem beliebigen Quellsystem eintreffen, liefert es Ermittlern den nötigen Kontext und das Verständnis, selbst wenn die Daten begrenzt, knapp oder sogar irreführend sind.

Auch das IBM i2 Analyst's Notebook ist bei der Strafverfolgung ein wichtiges Hilfsmittel. Es handelt sich hierbei um eine visuelle Analyseumgebung, mit der Analysten schnell mit aufgelösten Daten aus InfoSphere Identity Insight und mit importierten Daten aus anderen Quellen arbeiten können. Dank der erweiterten Darstellungsfunktionen des i2 Analyst's Notebook können Analysten und Ermittler wichtige Personen, Ereignisse, Verbindungen, Muster und Trends leichter identifizieren und so das Verständnis für die Struktur, Hierarchie und Vorgehensweise krimineller Netzwerke verbessern. Dies ermöglicht zeitnahe und präzise operative Entscheidungen, da sich die Kommunikation komplexer Daten aus unterschiedlichen Datenquellen vereinfacht.

Die nahtlose Integration von InfoSphere Identity Insight und des i2 Analyst's Notebooks erhöht die Produktivität, Genauigkeit und Vollständigkeit von Untersuchungen, da Verbindungen zwischen Unterlagen über Identitäten, Beziehungen und komplexen Ereignissen im Voraus berechnet werden, sodass eine sofortige Darstellung in Echtzeit und weitere Analysen möglich sind.



유승현	RYOO YONG WON	유경옥	YOO JUNG OK
유원술	YOO WOL CHOOL	유정웅	YU JEONG W.
유은경	YOO YOON S.	유정자	YOO CHONG CHA
유익희	RYU IK HIE	유정주	RHYU JEONG JOO
유인구	YU IN GOO	유정현	YU CHONG IL
유인국	YU IN GOOK	유정호	YOO JUNG HO
유인덕	YOO IN DUK	유정환	YOO JUNG HWAN
유인상	YOO IN SANG	유제연	LEW JANE Y.
유인성	LYU IN SANG	유종구	YOO JONG GU
유인상	YOO IN SANG	유종덕	YOU JONG DEUK
유인태	LYU IN TAY	유종수	YOO JONG SOO

Abbildung 2: Dieses Beispiel einer Seite aus einem koreanisch-amerikanischen Telefonbuch in Nord-Virginia zeigt mehrere Nachnamen, die tatsächlich abweichende Schreibweisen desselben Namens sind, wie die übereinstimmenden koreanischen Zeichen in den linken Spalten zeigen. Je nach Kultur kann ein Name viele Eigenschaften (Titel, Spitznamen usw.) aufweisen, die von einer intelligenten Verarbeitungsfunktion wie InfoSphere Global Name Recognition automatisch verstanden werden.

Höhere Effizienz von Untersuchungsverfahren

Für Strafverfolgungsbehörden ergeben sich durch diese fortschrittlichen IBM Tools, die auf Folgendes ausgerichtet sind, mehrere Vorteile:

- Ermittler müssen weniger häufig zahlreiche Suchvorgänge über mehrere Datenquellen hinweg durchführen
- Ganzheitliche Ansichten von Einheiten, da alle Informationen an einem Ort gesammelt werden
- Vorabrechnung schwieriger Verbindungen zwischen den Einheiten zur sofortigen Analyse
- Geringeres Risiko, dass ereignis- oder personenbezogene Informationen oder Beziehungen fehlen und Untersuchungen unterbrochen werden müssen
- Höhere Sicherheit und besseres Situationsbewusstsein der Mitarbeiter durch Benachrichtigungen über Ereignisse und Beziehungen, die ihnen nach routinemäßigen Abfragen und Suchvorgängen üblicherweise nicht zur Verfügung stehen

Das System aktualisiert Identitäten und Beziehungen automatisch und kann Benachrichtigungen senden, um sicherzustellen, dass die Ermittler immer über die neuesten Informationen zu einem Fall verfügen. Durch diesen Prozess erhöht sich die Produktivität der Ermittler und er hilft ihnen dabei, schnell Erkenntnisse für die Lösung von Fällen zu gewinnen.

Die Tools nutzen darüber hinaus Anwendungsprogrammierschnittstellen (APIs), um viele bestehende Quellsysteme zu integrieren, riesige Datenmengen aufzunehmen und dennoch eine Leistung nahezu in Echtzeit zu bieten. Sie nutzen außerdem Funktionen auf dem InfoSphere Information Server, um die Daten zu verstehen, zu bereinigen, zu transformieren und bereitzustellen, die hervorragende Analysen ermöglichen.

Untersuchungserkenntnisse in der Praxis

Wie in vielen Strafverfolgungsbehörden gab es auch in einer bekannten nordamerikanischen Polizeibehörde mehrere, unterschiedliche und nicht miteinander verbundene Systeme, auf denen Informationen über die Aktivitäten von Verdächtigen, verurteilten Verbrechern, Banden und anderen gesuchten Personen und Organisationen gespeichert wurden. Die Ermittler mussten auf jedes System separat zugreifen und Informationen manuell einbinden – ein langwieriger, arbeitsintensiver Vorgang, der die Beamten von anderen Aufgaben abhielt.

In einigen Fällen wurden Informationen auf den Quellsystemen falsch eingegeben oder von Verdächtigen falsch gemeldet, was die Verknüpfung von Identitäten zwischen den Systemen für die Ermittler noch schwieriger machte. Die Polizeibehörde musste das Suchen und Einbinden von Informationen vereinfachen, um eine vertrauenswürdige Sicht auf jede an einer Untersuchung beteiligte Person zu erhalten.

Die gewünschte Lösung sollte Daten analysieren, Identitäten auflösen und es den Verantwortlichen ermöglichen, neue Erkenntnisse über die Beziehungen zwischen den Informationen zu gewinnen und Anhaltspunkte liefern, die zur Lösung von Fällen beitragen. Mit der Software auf dem IBM i2 Analyst's Notebook und vorab integrierten Daten aus IBM InfoSphere Identity Insight können die Ermittler jetzt Untersuchungen zu beliebigen Kriminalfällen beliebigen Umfangs durchführen.

Heute kann ein einzelner Ermittler der Polizeibehörde innerhalb weniger Minuten die Vorgänge durchführen, für die zahlreiche Mitarbeiter bisher mehrere Stunden oder Tage brauchten. Das System löst automatisch stündlich Daten auf und verarbeitet derzeit durchschnittlich 7.000 neue Datensätze pro Tag. Die Abteilung erreicht dadurch eine Komprimierungsrate von 40 Prozent bei Identitäten in den vorhandenen Daten. Gleichzeitig hilft das System den Ermittlern, bisher unbekannte Beziehungen und Verbindungen aufzudecken. In einem Fall konnte z. B. eine neue Bande identifiziert werden, da mithilfe vorab integrierter Daten aus InfoSphere Identity Insight Informationen aus Nachrichtenberichten schnell bestätigt und ausgeweitet werden konnten.

Durch das Erstellen einer ganzheitlichen Sicht auf Entitäten und Beziehungen mit InfoSphere Identity Insight und der Software des i2 Analyst's Notebooks können Strafverfolgungs- und Sicherheitsbehörden dazu beitragen, die Effizienz ihrer Mitarbeiter zu steigern, Fälle schnell zu lösen und Rückstände abzuarbeiten.

Darüber hinaus sorgt diese Strategie für das beste Ergebnis, ein sichereres Umfeld für Mitarbeiter in Strafverfolgungsbehörden und die Bürger.

Weitere Informationen

Wenn Sie mehr über IBM InfoSphere Identity Insight, das i2 Analyst's Notebook und andere IBM Lösungen erfahren möchten, die Organisationen für die öffentliche Sicherheit unterstützen, besuchen Sie uns unter:

ibm.com/id-en/marketplace/infosphere-identity-insight



IBM Deutschland GmbH

IBM-Allee 1
71139 Ehningen
ibm.com/de

IBM Österreich

Obere Donaustraße 95
1020 Wien
ibm.com/at

IBM Schweiz

Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Die IBM Homepage finden Sie unter:

ibm.com

IBM, das IBM Logo, ibm.com, Analyst's Notebook, i2 und InfoSphere sind eingetragene Marken der IBM Corporation in den USA und/oder anderen Ländern. Weitere Produkt- und Servicenamen können Marken von IBM oder anderen Unternehmen sein. Eine aktuelle Liste der IBM Marken finden Sie auf der Webseite „Copyright and trademark information“ unter: ibm.com/legal/copytrade.shtml

Dieses Dokument ist zum Datum seiner Erstveröffentlichung aktuell und kann jederzeit von IBM geändert werden. Nicht alle Angebote sind in jedem Land verfügbar, in dem IBM tätig ist.

Alle hier beschriebenen Kundenbeispiele dienen lediglich zur Veranschaulichung. Die tatsächlichen Leistungsergebnisse können je nach Konfiguration und Betriebsbedingungen variieren. Der Benutzer ist dafür verantwortlich, den Betrieb von Produkten oder Programmen anderer Anbieter in Verbindung mit IBM Produkten und Programmen zu prüfen und zu verifizieren. Vertragsbedingungen und Preise erhalten Sie bei den IBM Geschäftsstellen und/oder den IBM Business Partnern. Die Produktinformationen geben den derzeitigen Stand wieder. Für IBM Produkte gelten die Gewährleistungen, die in den Vereinbarungen vorgesehen sind, unter denen sie erworben werden.

© Copyright IBM Corporation 2019



Bitte der Wiederverwertung zuführen