Politique de sécurité publique : du “ détecter et réagir ” au “ prédire et agir ”

Sommaire :

1 Introduction
2 Applications de l’analyse prédictive
7 Autres applications
7 Conclusion
8 A propos d’IBM Business Analytics

Introduction

Aujourd’hui, les agences gouvernementales sont confrontées à de nouveaux enjeux de taille. En plus d’assurer la sécurité des populations et de combattre la criminalité et la violence en bandes, elles doivent assumer la lourde tâche de lutter contre le terrorisme et de contrôler les épidémies de maladies infectieuses.

Pour relever ces défis, les autorités tentent différentes approches. Les technologies de l’information innovantes jouent un rôle essentiel dans l’amélioration de notre capacité à anticiper les événements et à agir en conséquence. L’analyse prédictive est l’une d’entre elles.

L’analyse de l’information est la pierre angulaire d’une politique de sécurité publique efficace. L’objectif des activités de veille est de détecter à temps les menaces pour la sécurité, afin de pouvoir prendre les mesures appropriées. Or les modèles qui permettent d’identifier ces menaces sont souvent noyés dans une masse de données. Pour y parvenir, il existe une nouvelle forme d’analyse de l’information particulièrement utile : l’analyse prédictive.

Les solutions d’analyse prédictive appliquent des techniques statistiques, d’exploration de données et d’apprentissage automatique élaborées aux informations historiques afin d’aider les agences gouvernementales à identifier des schémas et des tendances cachés, même dans des ensembles de données étendus et complexes. Il peut s’agir aussi bien d’énormes tableaux de données structurées que de gros volumes de données textuelles, y compris des échanges par e-mail ou lors de conférences électroniques, dont les agences doivent évaluer les données. Grâce à l’analyse prédictive, vous pouvez anticiper quels types d’intervention seront nécessaires, et à quel niveau. Vous pouvez donc prévoir, au lieu de réagir, et tirer le meilleur profit des ressources disponibles.

Contrairement aux méthodes de détection et d’analyse à base de règles, l’analyse prédictive permet d’identifier des comportements assez inhabituels, même ceux présentant des différences subtiles qui manquent souvent à d’autres méthodes. Les techniques d’analyse prédictive consistent à explorer et tirer les enseignements de toutes les dimensions de données, permettant ainsi aux analystes d’allier connaissances humaines, première expérience et intuition pour guider leur application des techniques d’analyse. La capacité de l’analyse prédictive à combiner en permanence une grande variété de dimensions, types et sources de données permet de détecter rapidement et de manière fiable les signatures involontaires de pirates informatiques, de criminels ou de terroristes.

Points clés

- Utilisez l'analyse prédictive pour renforcer la sécurité aux frontières et le maintien de l'ordre, améliorer la détection des menaces d'intrusion, le contrôle des maladies infectieuses et la détection des activités de blanchiment de capitaux et de financement du terrorisme.
- Découvrez des modèles cachés et développez de nouvelles connaissances grâce à de gros volumes de données structurées et non structurées.
- Utilisez les modèles prédictifs pour anticiper les menaces, identifier les individus suspects et affecter les ressources adéquates de manière efficace.
- Créez un processus automatisé de création de modèles capables d'analyser les données propres à certains lieux.

Grâce à l'analyse prédictive, vous pouvez fonder vos décisions opérationnelles quotidiennes sur des modèles guidés par les données décrivant de façon précise les conditions actuelles et en développement. Vous pouvez ainsi :

- améliorer vos capacités de prévention et réduire les coûts de contrôle en déployant le personnel là où il est le plus utile ;
- prédire quels types d'événements sont les plus susceptibles de monter en puissance afin de prévenir cette montée en puissance ;
- mener de nouvelles investigations plus efficacement ;
- découvrir des schémas dans vos données qui vous incitent à approfondir vos recherches dans certains domaines ;
- explorer les menaces pour la sécurité et étudier les individus et les organisations concernés ;
- fournir des informations au secteur concerné, à l'endroit et au moment opportuns.

Applications de l'analyse prédictive

Sécurité aux frontières

Se protéger des menaces commence souvent aux frontières, dans les aéroports et dans les ports. Savoir prédire quels conteneurs entrant dans un port pourraient contenir des matières indésirables/dangereuses ou quels passagers d'une compagnie aérienne mériteraient d'être surveillés plus attentivement, ou encore savoir identifier les véhicules suspects aux frontières, sont les principales missions des agences de protection des frontières.

Ainsi, un grand pays a mis en place le scénario suivant avec la solution d'analyse prédictive IBM SPSS. La meilleure façon de décrire l'enjeu aux frontières de ce pays est la suivante :

" Nous ne pouvons pas intercepter et fouiller chaque véhicule qui passe la frontière. En revanche, si nous pouvions prédire avec précision le niveau de risque associé à chaque véhicule – qu'il transporte des produits de contrebande, de la drogue, de l'argent, des armes ou des clandestins, nous pourrions tirer le meilleur parti de notre personnel d'inspection, accroître nos taux de détection, mieux protéger le pays et ses habitants et améliorer l'expérience des voyageurs innocents en accélérant leur passage à la frontière. "

A chaque frontière, des caméras enregistrent et reconnaissent le numéro d'immatriculation de chaque véhicule. Une fois le véhicule identifié, des consignes s'affichent sur les écrans du poste frontière, indiquant aux contrôleurs de laisser passer le véhicule ou de le diriger vers le deuxième poste de contrôle. Si un véhicule doit subir une deuxième inspection, des informations sont envoyées sur l'assistant électronique de poche de l'inspecteur chargé de l'affaire, indiquant la probabilité de chaque type de risque (drogue, armes, etc.) et donnant des conseils sur ce qu'il doit rechercher.

Les véhicules sélectionnés, les évaluations des risques et les résultats des contrôles sont ensuite enregistrés pour permettre d'établir un reporting continu sur les niveaux d'inspection par type de risque, les taux de réussite, les taux de faux positifs et le volume et la valeur des saisies.

Enfin, des modèles sont créés à partir des résultats de ces contrôles passés. Les données utilisées sont classées par numéro d'immatriculation et incluront le type de véhicule (dimensions, capacités, etc.), le nom du propriétaire du véhicule (et par conséquent toutes les informations disponibles sur le propriétaire ou le conducteur), et l'historique des passages aux frontières du véhicule, à ce poste frontière ou à un autre. D'autres critères donnant des indications sur le passage de la frontière pourront également être ajoutés, tels que le jour de la semaine, l'heure et les conditions météorologiques dominantes.

Un modèle est créé par type de risque. Afin de transformer les scores de chaque modèle en actions, ceux-ci seront associés à des règles représentant le meilleur niveau de connaissance humaine sur l'évaluation des risques. Certaines de ces règles contribueront à déterminer le niveau de précision avec lequel les véhicules contrôlés seront sélectionnés (et par conséquent le type de risque entraînant une deuxième inspection) et pourront varier selon le niveau de connaissance prédéfini des pics de trafic, ou être ajustées manuellement en cas de trafic anormalement élevé afin d'éviter l'accumulation des deuxièmes contrôles en attente.

L'agence concernée contrôle environ 300 postes frontières, et même si nombre d'entre eux affichent des schémas de violation similaires, chacun possède son propre profil indiquant les risques probables ainsi que les tentatives d'infraction et les méthodes utilisées. Idéalement, chaque poste frontière devrait avoir son propre modèle pour chaque type de risque, établi à partir de données locales. Créer et gérer manuellement tous ces modèles exigerait de nombreuses ressources, coûterait cher et serait peu pratique. Si, en revanche, des experts en analyse créaient un processus automatisé de création et d'application des modèles, celui-ci pourrait être appliqué efficacement aux données locales pour chaque passage de frontière et représenterait la " solution optimale " incarnant les meilleures pratiques nationales.

Maintien de l'ordre

En matière de maintien de l'ordre, les tendances au comportement suspicieux ou criminel peuvent être identifiées à l'aide d'une multitude d'informations, y compris des données agrégées ou des données d'incidents. Ainsi, un analyste criminel peut utiliser l'analyse prédictive pour :

- identifier les zones habituellement fréquentées par les criminels violents,
- rapprocher les tendances régionales ou nationales en matière d'activité des bandes des incidents locaux,
- établir un profil des crimes pour repérer les similitudes et rapprocher les crimes de délinquants connus,
- identifier les circonstances (manifestations en ville, conditions météorologiques, vacances, etc.) les plus susceptibles de déclencher des crimes violents afin de prédire où et quand ces crimes risquent de se reproduire à l'avenir.

Les organismes de sécurité publique s'appuient sur des données provenant de différentes sources et applications. C'est pourquoi les solutions d'analyse prédictive basées sur une architecture ouverte sont particulièrement intéressantes : elles produisent des résultats rapidement à partir des données existantes. Mais l'analyse prédictive produit vraiment ses effets lorsque les modèles et les analyses prédictives sont livrés aux utilisateurs en amont – les officiers en patrouille, les inspecteurs en charge d'une affaire et leurs responsables.

Le personnel en amont n'a pas besoin de comprendre la technologie pour profiter des résultats de l'analyse prédictive. Ils peuvent accéder aux informations prédictives dans un format facile à comprendre et à utiliser, directement depuis un navigateur.

IBM compte des centaines de clients dans le monde au sein des organismes de sécurité publique, des appareils judiciaires, des établissements pénitentiaires et des commissions chargées des libérations conditionnelles au niveau local, régional et national. Ils utilisent tous le logiciel IBM SPSS à des fins multiples :

- analyse des informations historiques pour mieux prévoir les tendances en matière de criminalité,
- prévision des besoins d'établissements correctionnels en fonction des tendances en matière de taux de criminalité,
- évaluation du succès des programmes de réhabilitation,
- sélection de l'implantation géographique des centres de commandement de l'état d'urgence selon la fréquence et le lieu des incidents,
- analyse des preuves médico-légales (numériques),
- identification des réseaux criminels et terroristes à partir des données de surveillance, de communication et Internet,
- établissement du profil des crimes, des criminels et des scènes de crime,
- prédiction de l'efficacité du déploiement des ressources,
- identification rapide des modèles à partir des données des affaires très médiatisées.

Détection des menaces d'intrusion

Les coûts liés à l'attaque d'une personne malveillante, qui accède ainsi à des informations privilégiées (d'initiés), auront souvent un impact fort et durable : violation de la confidentialité, atteinte à l'intégrité de l'information, influence néfaste sur la politique du gouvernement, révélation des sources et des méthodes et compromission des opérations de terrain.

Menaces internes

Les cybercrimes d'initié sont souvent très difficiles à détecter car l'auteur du crime a souvent un motif légitime pour accéder, modifier et manipuler des données critiques et/ou sensibles. Malgré ces difficultés, la plupart des organisations disposent d'un volume de données substantiel qui peut servir à caractériser et potentiellement limiter les effets d'une attaque par un initié malveillant. Il peut s'agir de données démographiques, d'évaluations des performances, de missions existantes ou passées, de communications électroniques internes et externes et de fichiers journaux.

Si une entreprise ou une agence est attentive à l'accès des initiés aux données sensibles, elle utilisera très souvent un ensemble de règles codées en dur pour identifier les comportements potentiellement anormaux. Par exemple, elle demandera à ce qu'une personne qui travaille normalement sur des dossiers de ressources humaines soit contrôlée si elle tente à plusieurs reprises d'accéder à des fichiers contenant des données sensibles du service Ingénierie. Les opérations potentiellement malveillantes sont cependant souvent beaucoup plus subtiles et difficiles à détecter.

Une méthode de détection des menaces d'initié par l'analyse prédictive consiste à prendre des cas connus de comportement malveillant et à caractériser les différences entre ces cas précis et les cas " normaux " connus. Bien qu'il s'agisse là d'une approche idéale, dans le sens où les algorithmes prédictifs permettent de reconnaître rapidement et facilement un comportement passé, il existe des difficultés inhérentes à l'utilisation exclusive de cette approche. D'une manière générale, les opérations d'initié malveillantes sont très rares. Les données historiques permettant de modéliser un comportement futur manquent souvent de cas d'illustration pour prédire précisément les cas similaires mais pas exactement identiques aux précédents cas connus d'opérations malveillantes.

Lorsqu'il s'agit de menace interne ou détection de fraude, on se rend compte qu'une personne malveillante peut afficher des schémas comportementaux normaux, dynamiques et complexes. Dans ce cas, le délit peut être très difficile à détecter car le comportement de cette personne peut continuer à sembler légitime, et ne laisser transparaître que quelques légères évolutions au fil du temps. Il est donc important de déterminer non seulement le type de comportement affiché par les individus, mais aussi les individus dont le comportement diffère légèrement de celui de leurs homologues, ou a récemment évolué.

La technologie IBM SPSS propose plusieurs méthodes automatiques de détection des anomalies. Cela est particulièrement utile pour les travaux de veille car le processus peut être automatisé et permettre ainsi aux analystes de passer au peigne fin des millions d'enregistrements afin d'identifier les comportements atypiques ou les anormalités.

Très souvent, la meilleure approche de l'évaluation des risques en interne regroupe plusieurs méthodes idéalement adaptées aux objectifs spécifiques de l'agence et aux données disponibles. Il est important de commencer par déterminer les objectifs et les problèmes potentiels découlant de l'analyse. Si l'on évalue et réduit la menace potentielle d'une attaque d'initié, ces objectifs peuvent être les suivants :

- déterminer une prédiction, un niveau de confiance et la propension au risque d'attaque d'initié,
- calculer le coût ou l'impact prévu de la violation de l'information,
- identifier l'ampleur et le périmètre d'une attaque dans les cas où la perte ou le coût de l'information n'est pas quantifiable,
- prioriser les audits des anomalies ou des menaces détectées en fonction du niveau de risque et des ressources disponibles pour mener l'enquête.

Menaces externes

Les techniques d'analyse des menaces internes sont également souvent utiles pour l'analyse des menaces externes. La principale différence entre l'analyse des menaces internes et l'analyse des menaces externes concerne la disponibilité des données. Les attaques provenant de sources externes fournissent rarement le type de données démographiques disponibles pour l'analyse des menaces internes. Les champs de données, tels que l'âge, l'appartenance à un groupe, la situation géographique et les schémas comportementaux historiques qui peuvent être attribués à un individu ou à un groupe sont beaucoup plus difficiles à obtenir lorsque vous analysez des menaces externes.

Lorsque les menaces externes ne fournissent pas suffisamment d'informations sur l'individu ou le groupe responsable d'une attaque ou d'une attaque potentielle, l'utilisation des techniques d'analyse des réseaux sociaux (SNA – Social Network Analysis) peut aider les enquêteurs à mieux évaluer le risque d'une menace externe spécifique en faisant des associations avec d'autres individus, groupes ou précédentes tentatives d'attaque connus.

Contrôle des maladies infectieuses

Pour assurer la protection sanitaire de ses concitoyens, une agence gouvernementale nationale utilise le logiciel d'analyse prédictive IBM SPSS Data Collection pour analyser la source et la propagation des maladies infectieuses, et pour se préparer et être capable de réagir dans l'urgence aux menaces pour la santé publique. Lorsqu'une épidémie de maladie infectieuse se déclare, il est impératif que l'agence regroupe rapidement des informations de santé publique, quel(le) que soit le lieu ou la cause de l'épidémie. Afin de mieux comprendre ces épidémies et de réagir plus efficacement, l'agence rationalise les retours d'information dans un environnement contrôlé et très sécurisé.

Elle peut obtenir des retours immédiats de la part des citoyens sur les informations de santé publique critiques, quel(le) que soit le pays ou la langue, à travers une multitude de canaux comme le téléphone, les entretiens en face à face et les sondages en ligne, ce qui lui permettra de mieux comprendre la maladie et de prendre les mesures les plus appropriées. Ces connaissances permettent à l'agence d'améliorer sa compréhension des problèmes de santé publique majeurs et ainsi de réduire le taux de morbidité et de mortalité des populations exposées aux maladies infectieuses.

Suite à une épidémie de pneumonie dans un lycée en 2007, l'agence a rapidement établi un questionnaire qui a été envoyé par e-mail à tous les étudiants afin d'obtenir des réponses rapides et détaillées sur les comportements, les actions et les éventuelles expositions au risque passés, dans le but d'identifier les cas potentiels non détectés. Les informations recueillies ont permis de caractériser la maladie et d'identifier les facteurs de risque liés à la maladie. L'agence a ainsi pu rapidement identifier l'étiologie de l'épidémie de pneumonie, informer tous les étudiants de la situation et diffuser des informations de prévention afin de stopper la propagation de la maladie.

Cette organisation utilise aussi le logiciel IBM pour évaluer les besoins médicaux de populations ciblées en cas de catastrophe naturelle. A l'occasion de plusieurs catastrophes majeures, l'agence a déterminé quels étaient les besoins médicaux (médicaments et matériel médical) des victimes.

Lutte contre le blanchiment de capitaux et le financement du terrorisme

Dans la lutte contre le crime organisé, le trafic d'êtres humains et le terrorisme, l'identification des opérations financières suspectes est une préoccupation majeure des agences d'investigation. Le vieil adage " Suivez l'argent " est toujours d'actualité.

Les solutions d'analyse prédictive offrent les fonctions élaborées de reconnaissance des formes, de détection des anomalies et d'analyse des risques nécessaires pour détecter avec succès les tentatives de blanchiment de capitaux. Elles permettent aussi de détecter le financement d'activités terroristes.

Grâce à elles, les enquêteurs peuvent :

- créer des profils d'activités financières passées,
- créer des groupes de pairs pour les comptes similaires,
- identifier les cas où les activités s'écartent de façon suspecte de ces profils ou groupes de pairs,
- limiter les faux positifs à l'aide de techniques de pondération basées sur les risques,
- repérer les activités suspectes et prendre rapidement les mesures adéquates.

Une banque commerciale réputée utilise le logiciel d'analyse prédictive d'IBM SPSS pour surveiller les modèles transactionnels de ses clients. La banque s'est engagée à prévenir toute activité de blanchiment de capitaux au sein de son organisation. Grâce à la technologie IBM SPSS, elle a pu réduire le nombre d'opérations qui exigeaient d'être contrôlées de plus de 90 %. Elle a même renforcé son degré de précision en identifiant des cas positifs de blanchiment de capitaux, aidant ainsi les enquêteurs à adapter facilement les modèles aux méthodes en constante évolution des responsables de ces activités criminelles.

La banque a également amélioré l'efficacité de son processus de vérification, le volume d'enquêtes dont les autorités ont été alertées étant passé de moins de 25 % à plus de 60 %. Enfin, la banque a réduit considérablement les coûts administratifs des enquêtes sur les opérations suspectes, qui ont baissé de 60 %.

Autres applications

La solution d'analyse prédictive IBM SPSS propose d'autres applications en matière de sécurité publique :

- surveillance des sites Internet pour détecter les recruteurs de terroristes et suivre leur activité,
- prédire les besoins de maintenance des ressources essentielles pour garantir une haute disponibilité,
- améliorer la conservation et le recrutement des ressources humaines cruciales.

Conclusion

La population compte sur votre service ou votre agence pour protéger sa santé et assurer sa sécurité. Pour le faire efficacement, vous devez mettre à profit votre personnel et vos autres ressources, le plus efficacement possible. Il est donc essentiel de disposer d'informations précises sur les situations présentes et passées. L'exploitation des données prédictives vous assure une plus grande maîtrise, ce qui permet à votre agence de déployer les ressources adéquates au bon endroit et au bon moment.

Assurer la sécurité d'une nation est une mission délicate et exigeante, qui exige une coordination des efforts de nombreuses agences. Le plus tôt votre agence obtiendra des informations fiables, le plus tôt vous pourrez élaborer des plans et prendre les mesures nécessaires. Que vous soyez chargé d'interpréter des données de veille, d'identifier des menaces internes, de vous protéger contre les attaques de réseaux ou d'infrastructures physiques, d'assurer la sécurité aux frontières ou de surveiller tout autre type d'activité menaçante ou suspecte, les solutions IBM SPSS peuvent vous aider à mieux protéger les individus qui comptent sur vous en transformant vos capacités de " détection et réaction " en capacités de " prédiction et action " .

A propos d'IBM Business Analytics

Les logiciels IBM Business Analytics aident les entreprises à mesurer, comprendre et anticiper leur performance financière et opérationnelle en fournissant des informations exactes, cohérentes et complètes. Ce portefeuille complet de solutions décisionnelles, d'analyse prédictive, de gestion des performances financières et des stratégies et d'applications d'analyse fournit une vision claire, immédiate et concrète des performances actuelles et permet de prévoir les résultats futurs. Alliant de riches solutions sectorielles, des services professionnels et les meilleures pratiques, il permet aux entreprises de toutes tailles d'optimiser leur productivité, d'automatiser en toute confiance leurs décisions et de générer des résultats supérieurs.

Faisant partie de ce portefeuille, la solution logicielle IBM SPSS Predictive Analytics permet aux entreprises de prévoir les événements et d'agir proactivement en fonction des données obtenues pour obtenir de meilleurs résultats métier. Les clients des secteurs privé, public et universitaire du monde entier font appel à la technologie IBM SPSS qui les dote d'un atout concurrentiel pour attirer, fidéliser et développer leur clientèle, tout en réduisant les fraudes et en atténuant les risques. En intégrant les logiciels IBM SPSS à leurs opérations quotidiennes, les entreprises deviennent proactives, capables de diriger et d'automatiser leurs décisions pour atteindre leurs objectifs métier et se doter d'un atout concurrentiel. Pour plus d'informations ou pour contacter un interlocuteur IBM, visitez le site **ibm.com**/spss/fr

Compagnie IBM France
17, Avenue de l'Europe
92275 Bois-Colombes Cedex

Business Analytics software

YTW03024-FRFR-01