Fraunhofer FKIE · DITS.center · Analytical Semantics · traversals

FIFI Fraud ▪ Information ▪ Fusion ▪ Intelligence

Ziele, Konzepte und assoziierte Partnerschaften

Wir danken der Initiative von Philip Morris International, das Projekt im folgenden Sinne maßgeblich zu fördern:

Combating illegal trade, together. A global initiative to support projects against illegal trade and related crimes.

PMI impact

Illegale Aktivitäten in jeglicher Form (Diebstahl, Schmuggel, Markenpiraterie etc.) bilden eine Herausforderung für den globalen Handel. Die Quellen, aber auch der konkrete Ablauf illegaler Handlungen sind dabei schwer zu identifizieren, zumal Bedrohungen sowohl von außerhalb als auch aus dem eigenen Unternehmen heraus auftreten.

Zusätzlich können auch Verstöße gegen unternehmensinterne Richtlinien unerwünschte und kostenträchtige Folgen haben.

Die Industrie verfolgt mit ihren Sicherheitsabteilungen solche Vergehen, um das Unternehmen vor Schaden zu bewahren. Damit wirksame Gegenmaßnahmen zielgerichtet erfolgen können, müssen Informationen, die auf diese illegalen bzw. unzulässigen Aktivitäten hindeuten können, erfasst und geeignet analysiert werden. Ziele sind die Aufklärung der Umstände, nach Möglichkeit die Prädiktion und Prävention oder auch die forensische Analyse von Vorfällen. Wie in hoheitlichen Behörden werden Informationen aufgenommen, verarbeitet, analysiert und zu Handlungsempfehlungen für das Management verdichtet.

Das Projekt FIFI dient der anwendungsnahen Forschung, um innovative Lösungen mit Leistungsmerkmalen zu schaffen, die zur Steigerung von Effektivität und Effizienz dienen. Technische Unterstützung der Analysten als auch die Leistung von Beiträgen zur Optimierung der Geschäftsprozesse sind Ziele für das Vorhaben.

Das Projekt wird als eines von 31 Projekten im Rahmen der Philip Morris Initiative IMPACT (second funding round) mit einem Volumen von ca. 1,5 Mio. US$ gefördert. Zusätzlich engagieren sich die Projektpartner mit der Einbringung verfügbarer Teillösungen.

Die folgende Präsentation erläutert die Motivation, die Zielsetzungen und auch insbesondere den Willen zur engen Kooperation mit der betroffenen Industrie, hoheitlichen Sicherheitsbehörden und Unternehmen, die Beiträge für geeignete Unterstützungsmaßnahmen und Assistenzsysteme für Sicherheitsbelange in ihrem Aufgabenfeld nutzen wollen.

Bitte sprechen Sie uns jederzeit an.

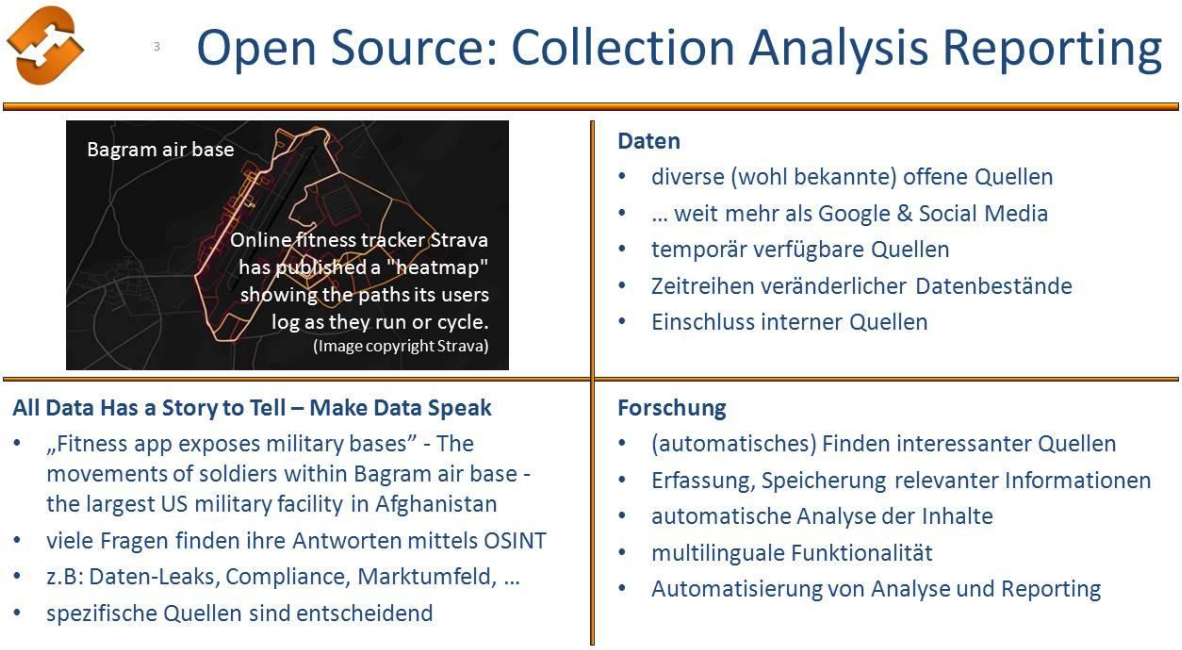
Dezember 2019

Der englische Begriff Intelligence im Kontext der systematischen Analyse und Beantwortung relevanter Fragen beschreibt ein Ergebnis und auch den Prozess, um hilfreiche Erkenntnisse zu gewinnen. Eine deutsche wörtliche Übersetzung gibt es nicht. „Wissen, was los ist“ soll als Leitlinie dienen, den englischen Begriff „Intelligence“ zu verstehen. Im Bereich hoheitlicher Einrichtungen spricht man auch von der Lage oder vom Lagebild.

Industrieunternehmen können neben den legalen, offenen Quellen auch auf interne Daten zurückgreifen, die aus Geschäftsprozessen, der Produktion und Lieferkette stammen. Daten werden nicht nur – aber auch – über Zahlen in strukturierter Form repräsentiert. Eine umfassende und vielfältige Ergänzung erfolgt durch unstrukturierte Informationen. Typischerweise sind diese Texte – ggf. auch in Audioform, Bilder und andere multimedial repräsentierte Informationen. Texte können in diversen Sprachen vorliegen, die sich einer Analyse nicht ohne Weiteres erschließen.

Wesentlich ist, dass die auszuwertenden Daten und Informationen möglichst umfassend sind und zur Fragestellung passen. Das Projekt verfolgt Lösungsansätze, um relevante Daten aus dem riesigen und unübersichtlichen Angebot, zielgerichtet zu ermitteln und der weiteren Bearbeitung zur Verfügung zu stellen. Die Transformation unstrukturierter Informationen in eine für den Analysten verständliche und interpretierbare Form ist Teil des Projekts; beispielhaft erwähnen wir die automatische Übersetzung fremdsprachlicher Informationen in die Zielsprache der Analystengruppe.

Die Gewinnung von Erkenntnis ist das Ergebnis eines Prozesses der Erfassung von Daten und Informationen sowie von deren Zusammenführung und Fusion. Diverse Maßnahmen sowie Technologien werden bei der zielgerichteten Analyse eingesetzt und führen schließlich zum Bericht zur Vorlage für die Entscheider. Entscheidend sind das Gespür und die Erfahrung der Analysten auch in Verbindung mit dem Einsatz technischer Unterstützungsmaßnahmen.

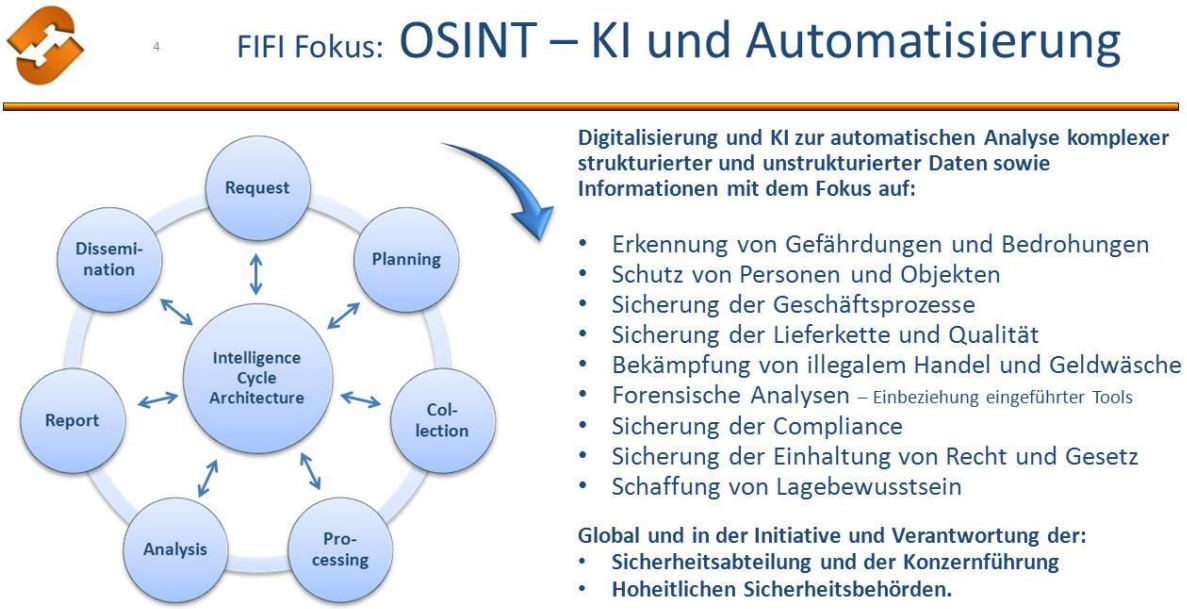


Open Sources bezeichnen hier alle frei und legal verfügbaren Daten und Informationen, die für eine Auswertung grundsätzlich zur Verfügung stehen. Der Begriff OSINT (Open Source Intelligence) steht für diese Kategorie von Informationen in Verbindung mit der Zielsetzung und Prozessen, um hieraus spezifische sowie relevante Erkenntnisse zu generieren.

OSINT ist ein Begriff, der seinen Ursprung in den traditionellen Vorgehensweisen hoheitlicher Sicherheitsbehörden hat. OSINT steht nicht für geheimnisvolle Prozesse unserer Sicherheitsdienste, sondern öffnet mit seinen Ideen und Prozessen Möglichkeiten, auch in der Industrie fortschrittlich und proaktiv im Sinne der organisationsbestimmten Sicherheitsstrategie agieren zu können.

OSINT ist nicht alleine die Verwendung von Google, um Material zu interessierenden Fragen zu beschaffen. Die kognitiven Fähigkeiten des Analysten, seine Fantasie und seine Ideen in Verbindung mit umfassender Erfahrung sind es, die Hinweise auf interessante Informationen liefern. Hierbei sind Quellen mit unerwartetem Potenzial und auch Quellen, die zeitlich nur beschränkt zur Verfügung stehen, von besonderem Interesse.

Offene Quellen, Diskussionsforen und auch Hinweise aus dem eigenen Unternehmen können helfen, geplante und noch nicht ausgeführte illegale oder unzulässige Handlungen zu erkennen und damit im Zusammenhang stehende Netzwerke zu erkennen. Eine möglichst große Vorwarnzeit, definiert als die Zeit zwischen dem Bekanntwerden eines bevorstehenden Ereignisses und dem Zeitpunkt seines Geschehens, ist entscheidend für erfolgreiche Gegenmaßnahmen zur Verhinderung illegaler Handlungen.



Die Gewinnung von Intelligence folgt einem Prozess, der seit Jahrzehnten in den einschlägigen Sicherheitsbehörden angewandt und trainiert wird. Ziel ist es, hoheitlichen Sicherheitsinteressen durch Informationen und Entscheidungsvorlagen zu dienen.

Der Prozess wird als Intelligence Cycle bezeichnet. In der Gemeinschaft der Anwender werden Varianten zum sequenziellen Prozess diskutiert. Es macht Sinn, diese Diskussionen zu verfolgen und auch im Hinblick auf die zivil und industriell orientierten Interessen zu prüfen.

Das Projekt soll helfen, Ereignisse zu vermeiden, die in der Vergangenheit für großes Aufsehen und in Folge für erhebliche wirtschaftliche Schäden gesorgt haben. Es ist nicht übertrieben von Informationskatastrophen zu sprechen, wenn die Wirkung von Compliance-Problemen, dem vermeintlich guten Willen der Techniker im Kontext mit beschönigten Produkteigenschaften, Schmuggel, Produktpiraterie und gefälschten Produkte betrachtet und bewertet wird.

Das Projekt dient nicht nur der forensischen Analyse von Vergehen, sondern vielmehr auch der Prädiktion und Prävention. Es soll Unterstützung bereitgestellt werden, um möglichst lange vor dem öffentlichen Bekanntwerden von problematischen Sachverhalten Handlungsspielraum für legale Gegenmaßnahmen zu eröffnen.

Neben der Vermeidung von Schaden dient Informationsaufbereitung auch der Verbesserung der strategischen Aufstellung des Unternehmens. Erkenntnisse zu Trends, Wettbewerberverhalten und der vom Markt wahrgenommenen Stellung des Unternehmens dienen einer kontinuierlichen Optimierung.

Im Folgenden stellen wir Use Cases dar, die wir im Rahmen des Projekts verfolgen wollen. Zusätzliche und alternative Fälle können wir berücksichtigen.

5

Use Case: Anomalien – in Lieferketten

Daten
- „Kaltstart" – Datenraum
- Streaming – Echtzeitdaten, aus:
  - Geschäftsprozessen
  - Open sources
  - Whistleblower („controlled")

Auftrag – Realtime Monitoring
- Tracking der Lieferkette
- fallbasierte Anomalie-Erkennung
  - Schmuggel, Betrug, Diebstahl
  - Wettbewerb, Informationsabfluss, Spionage
  - Produktfälschungen

Forschung
- Tracking der Lieferprozesse
- Modellbildung für den Normalfall
- Anomalie-Erkennung
- Datenmanagement – Massendaten
- Datenschutz (national – international)

6

Use Case: Analyse von „Daten-CDs"

Daten (statisch)
- Unternehmensdaten (Legal Sources)
  - Prozessinformationen
  - Kommunikation etc.
  - Massendaten
- Legal Open Source
- Whistleblower (controlled)

Auftrag an den Analysten (Team)
- Case Based (Corparate management controlled)
- Wahrung der Interessen der Beteiligten
- Aufklärung – Situationsbewusstsein
- Vermeidung von Überraschungen (Medien)
- Beispiel: Compliance Analyse

Forschung
- Verknüpfung un- & strukturierter Infos
- Massendaten (Speicherung, Verarbeitung)
- semantische Analyse (Text)
- ergonomische Assistenzfunktionen
- Automatisierung

7

Use Case: Anomalien – am Checkpoint

Daten

- Sensorik, Messungen, Röntgenbilder
- Fahrzeug- und Routendaten, Herkunft und Ziele
- Ladeunterlagen, Begleitpapiere, Personalpapiere
- OSINT, Wissensdatenbanken, Amtshilfe
- spezielle Quellen: Whistleblower, Spürhunde

Anomalie-Erkennung – Checkpoint Assistenzsystem

- Zielgruppe: Behörden der Zollverwaltung
- fallbasierte Anomalie-Erkennung
  - Schmuggel, Schleusungskriminalität
  - illegaler Handel, Finanzdelikte
  - Abgabenerhebung
  - Grenzsicherung

Forschung

- Modellbildung – Anomalie-Erkennung
- Vernetzung von:
  Quellen, Intelligence, Wissen
- Ergonomie von Apps und Endgeräten
- Datenschutz

8

Use Case: Geldwäsche

Daten

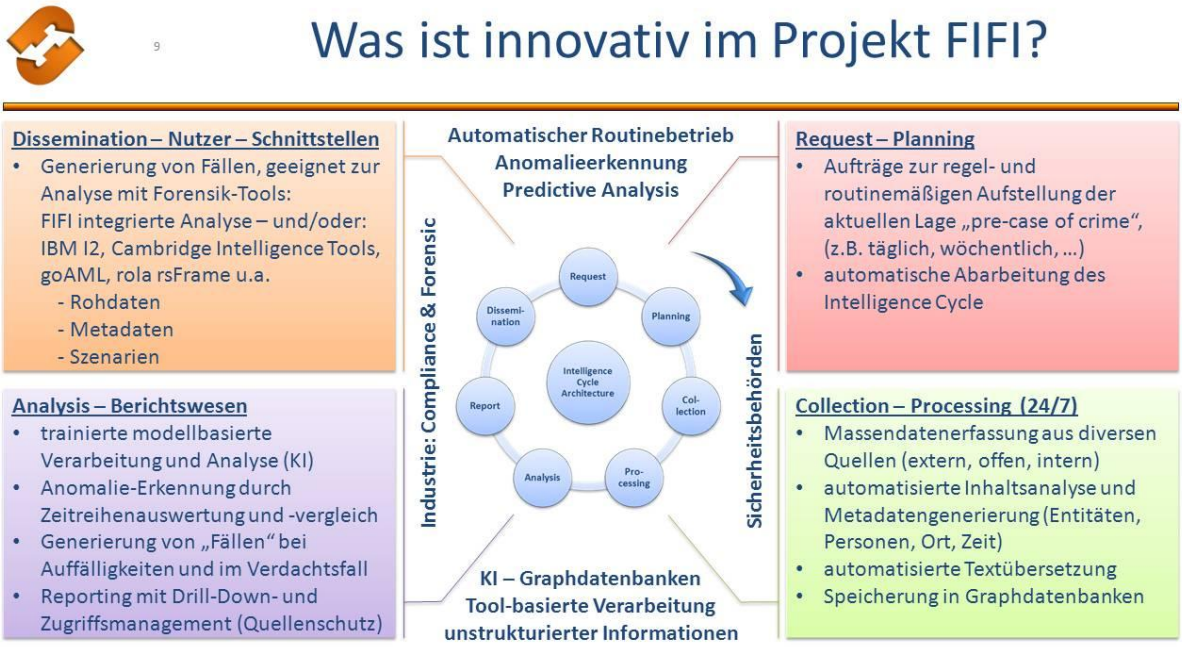
- Geldtransfer und Transaktionen, Meldungen
- Open Sources (Internet, Darknet), Social Media
- Kommunikation, E-mails, lawful Intercepts
- veröffentlichte Rechtsgeschäfte
- zugängliche Verträge, Notizen, Hinweise etc.

Aufträge zur Analyse –
Monitoringverfahren zur Identifikation von Fällen

- Zielgruppe: Behörden der Zollverwaltung, FIU
- fallbasierte Auswertungen von großen, statischen Datenbeständen (Panama, Offshore-, Lux-, Swiss-Leaks) als Ausgangspunkt für breit orientiertes Monitoring zur Anomalie-Erkennung (Tool NUIX)

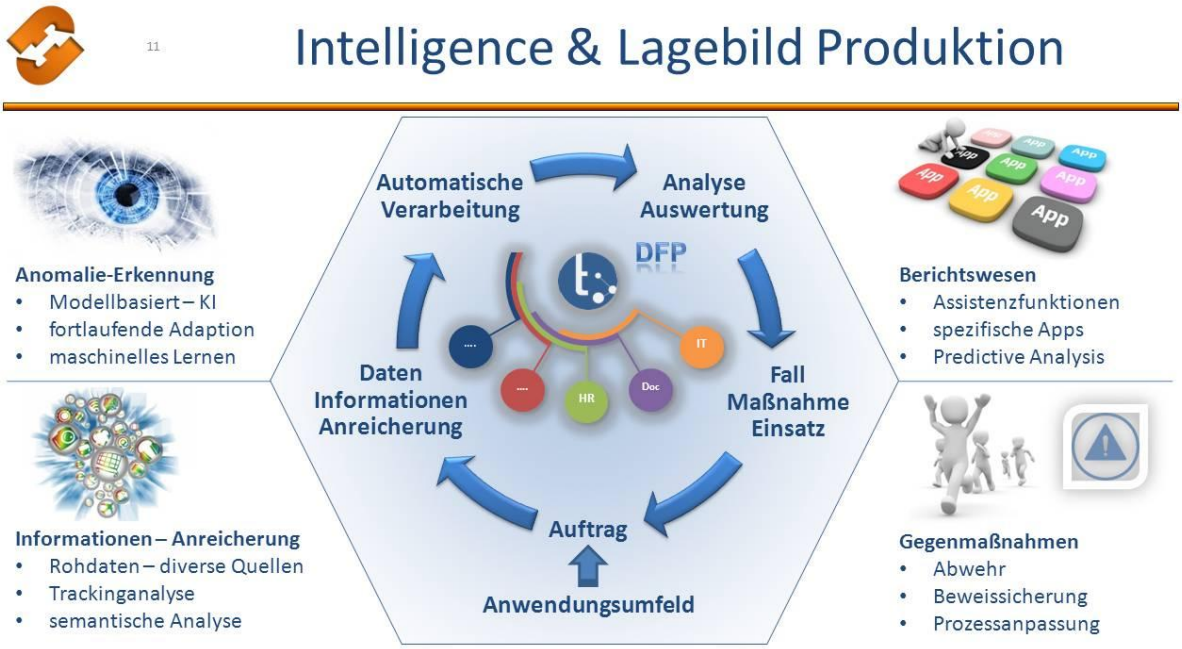
Forschung

- Modellbildung – Anomalie-Erkennung
- Verknüpfung von fallspezifischer Information mit Registern und offenen Quellen (Begleit-Info)
- Einsatz von KI im Monitoring von Massendaten
- Kooperation Forschung & FIU & Entwicklung



Innovation steht für eine Neuigkeit und dafür, dass der Markt keine solchen Lösungen zur Verfügung stellt. Im Projekt werden Ansätze verfolgt, die heute noch nicht frei erhältlich sind.

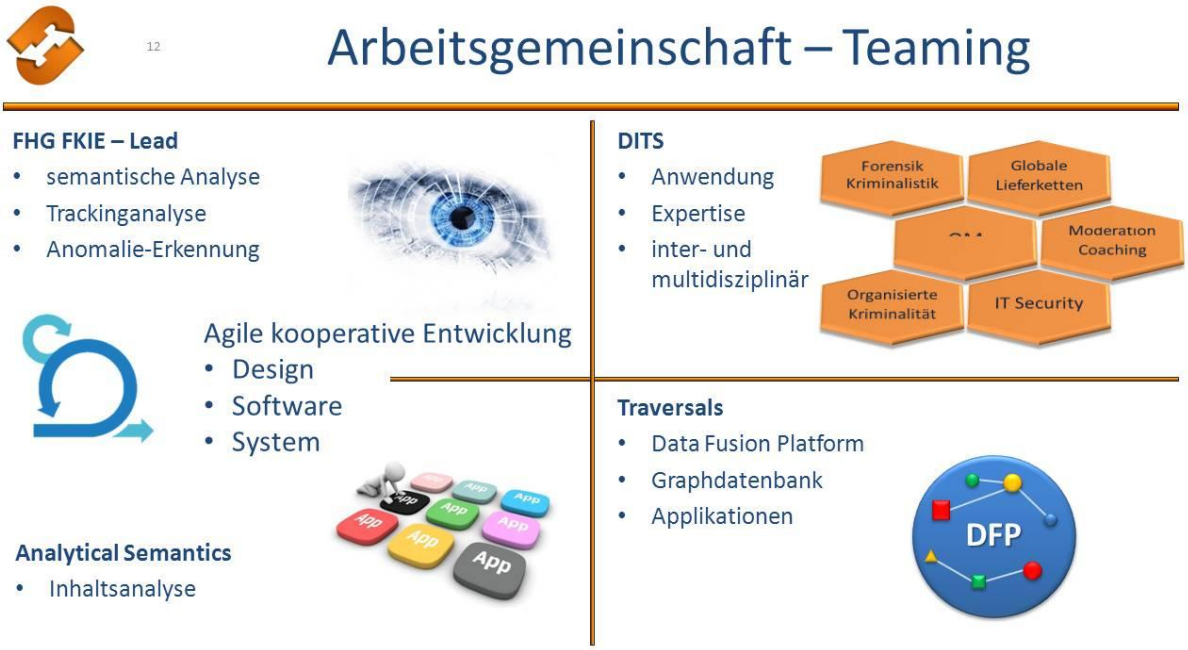
Auch ist zu bedenken, ob angebotene Lösungen unter gewissen Umständen zu einem unerwünschten und schädlichen Abfluss von Daten, Informationen, Erkenntnissen und geschäftsrelevanten Prozessen führen können. Wir berücksichtigen diese Aspekte und wollen gerne mit dem Anwender über wichtige Details sprechen und diese auch im Kontext von Anforderungen einbeziehen, die sich aus der Globalisierung ergeben.



Polizeien und hoheitliche Sicherheitsbehörden können Sicherheit für global agierende Unternehmen aus verschiedenen Gründen weder schaffen noch gewährleisten. Zum einen sind Vertraulichkeit und Öffentlichkeitsarbeit in Unternehmen anders definiert als sie durch staatliche Akteure verstanden werden. Zum anderen müssen im Bereich der Unternehmen zur Gewährleistung von Sicherheit Informationen auch über Landesgrenzen hinweg erhoben und verknüpft werden. Das ist für national agierende Sicherheitseinrichtungen problematisch, zumal bereits die Vernetzung und der darauf beruhende Informationsaustausch innerhalb der einzelnen Sicherheitseinrichtungen eines Staates nicht immer gegeben sind.

Sowohl Polizeien als auch hoheitliche Sicherheitsbehörden verfügen jedoch über eine große Erfahrung bei der Analyse von Daten. Zudem besitzen sie weitreichende Kenntnisse über die Methodologie und über Tools, um über die Datenerfassung und -analyse Erfolge zu erzielen.

Unser Ziel ist es daher, die bewährten Ansätze, Verfahren und Werkzeuge der Sicherheitsbehörden für die Belange der Sicherheitsabteilungen von Unternehmen anzupassen und nutzbar zu machen. Verknüpft mit dem technischen Wissen in der Analyse strukturierter und unstrukturierter Daten sowie den neuesten Entwicklungen im Bereich der künstlichen Intelligenz soll ein System entwickelt werden, welches aus den aufkommenden Massendaten, die z.B. innerhalb einer Lieferkette aufkommen, Unregelmäßigkeiten erkennt. Es soll dort eingesetzt werden, wo kaum kontrollierbare Datenbestände die Grundlage für den Eintritt eines Schadens darstellen können. Das System soll unterstützend bei der Erkennung von Anomalien in Datenströmen helfen.



Auf der Grundlage einer Förderung durch Philip Morris International im Rahmen des „PMI Impact“-Programms haben wir das Projekt „Fraud Information-Fusion Intelligence“ ins Leben gerufen. Unser Konsortium besteht aus dem Fraunhofer-Institut FKIE, DITS.center e.V., der Traversals GmbH und der Analytical Semantics AG.

Das FKIE, welches als Institut die Bundeswehr, die Bundespolizei, das BSI sowie diverse andere Sicherheitsbehörden berät, für diese forscht und Lösungen entwickelt, leitet das Projekt. FKIE ist inhaltlich mit seinen Abteilungen „Informationstechnik für Führungssysteme“ (ITF) und „Sensordaten- und Informationsfusion“ (SDF) beteiligt. Besonders die mit der auf die Auswertung von Textdokumenten spezialisierte Forschungsgruppe „Informationsanalyse“ der Abteilung ITF stellt ihre Expertise hier zur Verfügung.

DITS.center e.V. verfügt über ein Team von Experten aus allen Teilen des Sicherheitsbereichs, die mit ihrer Expertise Sicherheitsprojekte beratend begleiten.

Traversals ist darauf orientiert, „Intelligence as a Service“ anzubieten und die dafür geeigneten Werkzeuge mit dem Schwerpunkt auf der Auswertung offener Quellen in Verbindung mit intern verfügbaren Quellen zu entwickeln.

Analytical Semantics ist spezialisiert auf eine tiefe semantische Analyse von großen Datenmengen und bringt seinen einzigartigen Analyseansatz in das Projekt ein.

13

Assoziierte Partnerschaft – 2019 / 2021

Fraunhofer FKIE

DITS.center

Analytical Semantics

traversals

Anwender und Bezug zur Praxis
User Group

Ihre Mitarbeit als assoziierter Partner in den zwei Jahren der Projektlaufzeit bietet neue Erkenntnisse und Erfahrungen!

Wir berücksichtigen Ihre Anforderungen.

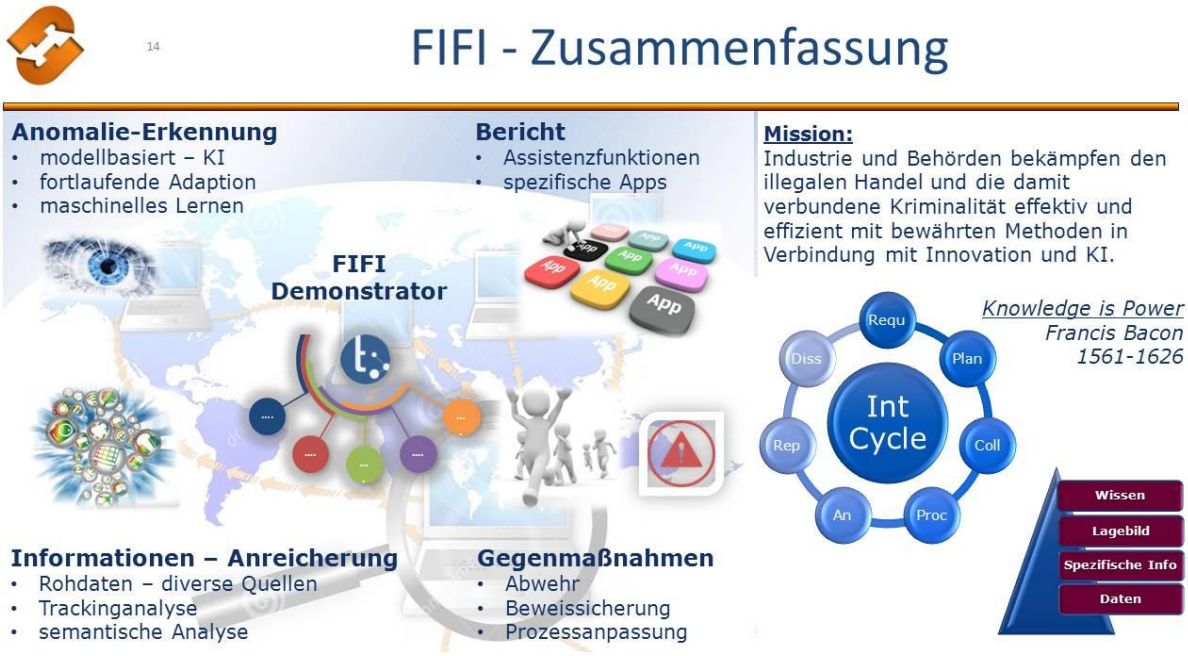
Ideal wäre es, wenn Sie Aufgaben und auch Daten einbringen.

Wir freuen uns darauf, gemeinsam mit Ihnen eine Lösung zu schaffen, die sich in der Praxis bewährt und Ihnen und Ihrem Unternehmen auch langfristig bei der Sicherung der Konzernsicherheit hilft.

Wir freuen uns über aktive Partner, die mit uns an den Aufgabenstellungen arbeiten wollen. Zusammen mit Ihnen identifizieren wir mögliche Schwachstellen innerhalb Ihres Unternehmens und versuchen Lösungen zu finden, um die Sicherheitslücken rechtzeitig zu erkennen und um einen möglicherweise entstehenden Schaden abzuwenden. Das auf Ihre spezifischen Anforderungen angepasste System, was Sie in Ihrer Arbeit unterstützen soll, stellen wir Ihnen selbstverständliche zu Verfügung.

Wir erwarten keine aktive Mitarbeit im Bereich der Forschung und Entwicklung. Wünschenswert ist die Teilnahme an regelmäßigen Workshops, die Mitwirkung bei der Erprobung von Lösungen und nach Möglichkeit die Bereitschaft, mit eigenen Daten zu testen oder diese für Testzwecke zur Verfügung zu stellen.

Für das Projekt würde eine solche Zusammenarbeit zur Evaluation der einschlägigen Methoden, Ansätze und Werkzeuge führen und den Erfolg des Projekts mitbestimmen.


14
FIFI - Zusammenfassung
Anomalie-Erkennung
• modellbasiert – KI
• fortlaufende Adaption
• maschinelles Lernen
Bericht
• Assistenzfunktionen
• spezifische Apps
FIFI
Demonstrator
Mission:
Industrie und Behörden bekämpfen den illegalen Handel und die damit verbundene Kriminalität effektiv und effizient mit bewährten Methoden in Verbindung mit Innovation und KI.
Knowledge is Power
Francis Bacon
1561-1626
Requ
Plan
Coll
Proc
An
Rep
Diss
Int Cycle
Wissen
Lagebild
Spezifische Info
Daten
Informationen – Anreicherung
• Rohdaten – diverse Quellen
• Trackinganalyse
• semantische Analyse
Gegenmaßnahmen
• Abwehr
• Beweissicherung
• Prozessanpassung

Notizen