



# Big Data Analyse im Gemeinsamen Lagezentrum für den Cyber- und Informationsraum

Oberstleutnant M.Sc. Dipl.-Ing. Thomas Erlenbruch  
KdoCIR Referatsgruppenleiter Analyseunterstützung

# Cyber- und Informationsraum

## Akteure



**Kriminelle**

**Innen-täter**



**Spione**



**Hack-tivisten**



**Staaten**



**Terror-isten**

لا إله إلا الله

رسول الله  
محمد

**Script Kiddies**

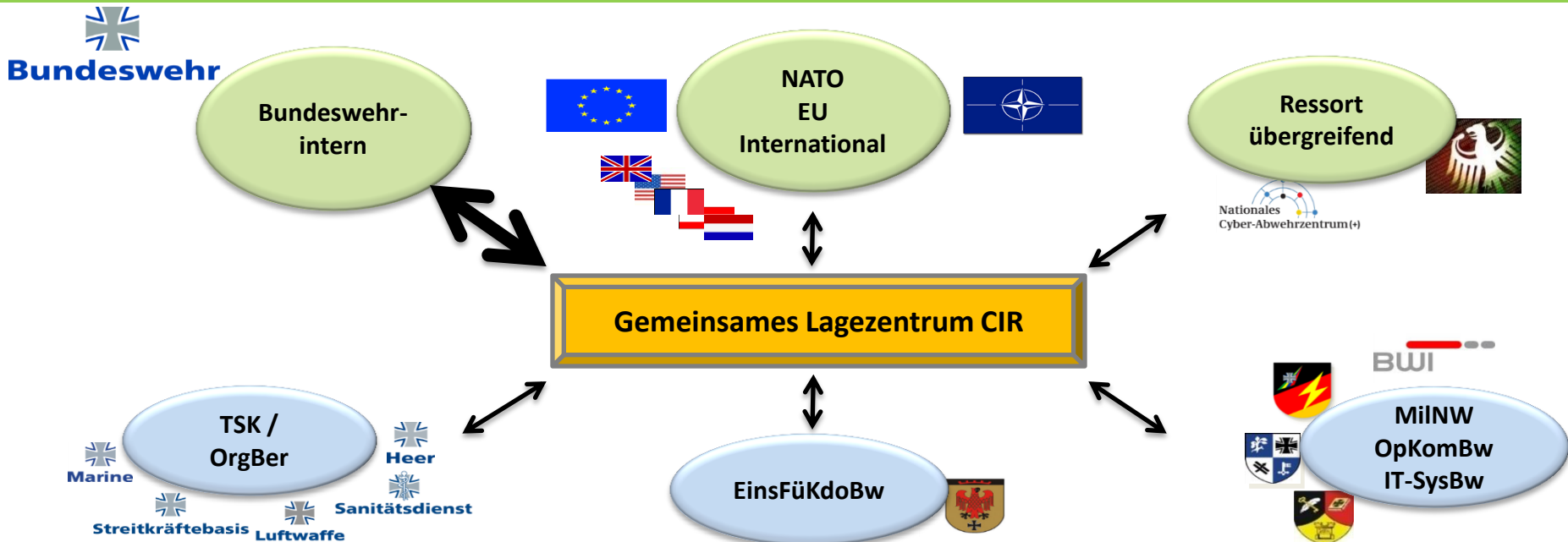




# Beziehungsgeflecht Gemeinsames Lagezentrum



## Bedarfsträger



## Teillagen



# Datenlieferanten



- Country Risk Daily Report
- Intelligence Weekly
- Terrorism & Insurgency Monitor
- World Insurgency and Terrorism
- Terrorism Watch Report
- Sentinel Security Assessment

Süddeutsche Zeitung



**dpa** Deutsche  
Presse-Agentur GmbH

**Frankfurter Allgemeine**  
ZEITUNG FÜR DEUTSCHLAND



**AP** Associated Press

**The New York Times**



Российская Газета  
**RGRU**

**العربية**  
Al Arabiya News Channel

**UPI.com**  
100 YEARS OF JOURNALISTIC EXCELLENCE

**ALJAZEERA**



# Big Data



We are drowning in information but starved for knowledge.

John Niasbitt



It is valuable, but if unrefined it cannot really be used. It has to be changed [...] to create a valuable entity that drives profitable activity.

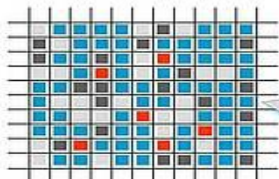
Clive Humby, UK Mathematician



# Standardanwendung

## STREAMING ANALYTICS

### BATCH PROCESSING VS. COMPLEX EVENT PROCESSING



**Batch Processing:** "Was war die durchschnittliche Temperatur der Maschine gestern?"

#### Data at Rest – Traditioneller Ansatz

- Store: Daten werden zuerst gespeichert
- Analyse: Dann werden die Daten verarbeitet



Analyse von Massendaten (in Echtzeit)

**Anomalien** nach denen gesucht wird **sind bekannt**



# Big Data Herausforderungen



## Volume:

schiere Anzahl an Daten

## Variety:

strukturierte, semi-strukturierte, unstrukturierte, Multimedia-Daten

## Velocity:

Auswertung in Echtzeit

## Value:

Steigerung des Unternehmenswerts (*Sicherheit im CIR*)

## Veracity:

Datenbestände liegen in unterschiedlicher Qualität vor.  
Bewertung der Aussagekraft.

Große Sets von Daten aus unterschiedlichen Quellen sind chaotisch und hässlich.  
Bill Franks



# Herausforderungen Datenmenge



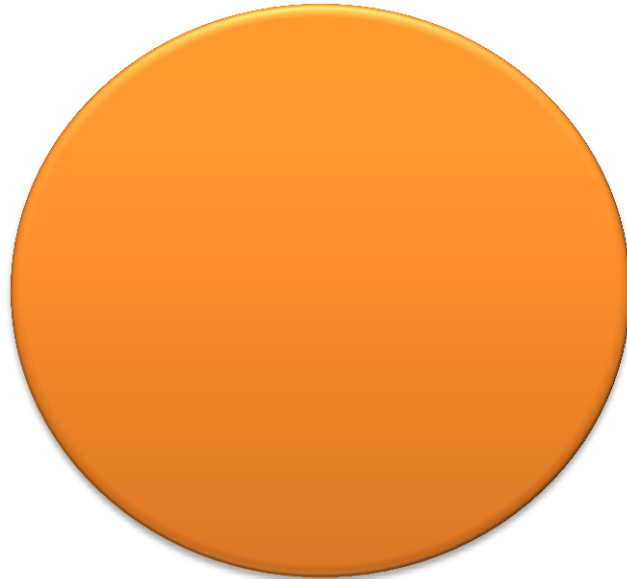
Teillagen  
Cyber/IT



Teillagen  
InfoR



IHS



Lexis Nexis



Twitter Thema IS





# Analyse

Verfahren im Gemeinsamen Lagezentrum



## Anomalieerkennung

Suche nach der unknown unknown.

**G**eografie

**P**olitik

**M**ilitär

**E**conomy

**S**ozial

**I**nfrastruktur

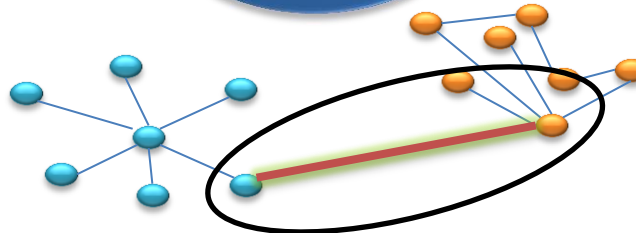
**I**nformation

Nat. Pers.  
Organisatio  
Malware  
Infrastruktur  
Geo  
...

Entitäten

IDOL  
VERTICA

Kategorien





# Dashboard Analysesoftware



KdoCIR  
Gemeinsames Lagezentrum

Dashboard

Übersicht und Statistiken

Übersicht  
Dashboard  
Dienstag, 10. April 2018

**Übersicht**

- Dashboard
- Themen
- Teillagen

**Analyse**

- Suche
- Bibliotheken
- Analysemappen
- Daten untersuchen
- Steckbrief
- Kollaboration

Version 1.2.0 PROD  
Aktualisiert am: 20.03.2018

**Betrieb**  
0  
Neue Dokumente

**CSOC**  
0  
Neue Dokumente

**OIG**  
1.401  
Neue Dokumente

**MilNw**  
0  
Neue Dokumente

**InfoU**  
0  
Neue Dokumente

**EigKr**  
0  
Neue Dokumente

Netzwerk des Tages

Netzwerk durchsuchen ...

🔍

Top Entitäten des Tages

Vorkommen	Entität
281	RUS
237	USA
143	CHN
76	Total
69	Donald Trump

Top Themen des Tages

Russische Föderation Letzte Aktualisierung April Bergel Lawrow  
Außenminister Bergel Lawrow letzten Jahr sagte am Dienstag Millionen Rubel Angela Merkel  
Russland Bereich Menschen Mont Stream



# Anzeige Dokument arabisch



KdoCIR  
Gemeinsames Lagezentrum

Übersicht

## Dokumentensuche

Dokumentenbasis mit komplexen Abfragen durchsuchen

Analyse  
 Suche

تایمز : شركات تحزّن البتكوين لدفع الفدية للقراصنة

📅 18.12.2017 12:19 UTC
🌐 Al Jazeera.net (OIG)
📄
📌
🔍

🔊 Offen
🏷️ Entitäten
🌐 ara

📄 Dokument
📄 Inhalt (ara)
🇬🇧 Englisch
🇩🇪 Deutsch

CIR-100088992

نقلت صحيفة تايمز البريطانية عن خبراء أن الشركات بدأت تفتح حسابات بعملة البتكوين الرقمية، وتخرّجها لتتغلق لقرصنة الإنترنت الذين يطالبون بفدية وتقوم الشركات بشراء هذه العملة لأنها تخفي برامج الفدية التي تسمح للبيانات من الحواسيب إذا فشل الضحايا في دفع رسوم البتكوين للمسئولين.

ومن المعلوم أن البتكوين عملة رقمية ليس لها شكل مادي، وهي توجد فقط كتسلسل من الرموز الرقمية، وقد زادت شعبيتها هذا العام بسبب تهافت جشرات الملايين من مستثمري القطاع الخاص في جميع أنحاء العالم عليها، مما رفع سعرها بنسبة 1800 %.

هذه رسوم بيانات الـ46 الحواسيب ما لم يتم دفع فدية بالبتكوين تعادل نحو 230 جنيه إسترليني من كل جهاز أصيب به. ولهذا السبب، ولجأ السبب (WannaCry) والجديس بالذكر أن نحو ثلث صناعات التوزيع التابعة للصحة البريطانية تعرضت للهجوم في مايو/أيار بفيروس فدية يسمى «تقوم الشركات بتخزين البتكوين تحسباً لدفع أي فدية».

إطلاق عقود البتكوين الأجلة في البورصات المنظمة خطوة نحو وضع هذه العملة الرقمية في النظام المالي السائد.

وكان من المقرر أن يبدأ التداول في عقود البتكوين الأجلة في شركة «سي إم إي غروب» ليلة أمس، بعد أسبوع من بدء مفاوضات «كبو غلوبل ماركتس» بيع عقودها من البتكوين.

والعقد الأجلة هي المنتجات المالية التي تسمح للتجار بالمراهنة على ما إذا كان سعر شيء ما سوف يرتفع أو يهبط على مدى فترة من الزمن، وتستخدم عادة لتداول الذهب والنفط والسلع الأخرى.

ويعتبر إطلاق عقود البتكوين الأجلة في البورصات المنظمة خطوة نحو وضع البتكوين في النظام المالي السائد. ومن أسباب ارتفاع سعر هذه العملة التوقّعات بأن عقود البتكوين الأجلة ستساعد البنوك الكبيرة والمؤسسات المالية الأخرى على دخول السوق.

وقد بلغ سعر البتكوين الواحد الليلة الماضية 18,950 دولاراً في بورصة بنسجام، التي تعتبر أفضل معيار للأسعار. ووصل سعره إلى أعلى مستوى له عندما سجل 19,666 دولاراً في بنسجام نهاية هذا الأسبوع.

وقد افتتحت لجنة تداول السلع الأجلة -التي تشرف على تداول العقود الأجلة في الولايات المتحدة- على خطط مجموعة كيو في بداية الشهر. وقال رئيس اللجنة إن البتكوين كان «سلمةً خلفاً لأي عملة تعاملت بها اللجنة في الماضي». وقال إن شركة دويتشه بورسي -المشغلة للبورصة الألمانية- تدرس تبادل العقود الأجلة للبتكوين.

Analyse

🔍 Suche  
📖 Bibliotheken  
🗺️ Analysemappen  
📄 Daten untersuchen  
📄 Steckbrief  
👥 Kollaboration

Version 1.16 PROD  
Aktualisiert am: 21.02.2018  
Nächste Version: 05.02.2018\*  
Warten auf 10.17.170.99...



# Anzeige Dokument arabisch Übersetzung DEU



K d o C I R  
Gemeinsames Lagezentrum

⚙️ ?

- Themen
- Teillagen
- Analyse**
- Suche
- Bibliotheken
- Analysemappen
- Daten untersuchen
- Steckbrief
- Kollaboration

**Version 1.16 PROD**  
Aktualisiert am: 21.02.2018  
Nächste Version: 05.03.2018\*  
(\* voraussichtlich)

تامز: شركات تخزن البتكون لدفع القدية للقر اصنة

📅 18.12.2017 12:19 UTC
📄 Al Jazeera.net (OIG)
📄
🗨️
🔍

📄 Dokument
📄 Inhalt (ara)
🇬🇧 Englisch
🇩🇪 Deutsch

🔊 Offen
👤 Entitäten
📄 ara
CIR-100088992

## Zeiten: Store albtwkn Unternehmen zu zahlen das Lösegeld Piraten

Die britische Times zitierten Experten, dass die Unternehmen begonnen, offene Rechnungen der Währung des digitalen albtwkn speichern, indem Sie das Internet Hacker, die Nachfrage ein Lösegeld. Unternehmen sind den Kauf dieser Währung, da er befürchtet die Programme der Lösegeld wischen Sie Daten vom Computer, wenn der Ausfall der Opfer in die Zahlung von Gebühren albtwkn Sneakers.

Es ist bekannt, dass albtwkn digitale Währung ist hier nicht die Form von Material, und es gibt nur kslasl Symbole Software, die Popularität erhöht hat in diesem Jahr wegen der Ansturm der Dutzende von Millionen von privaten Investoren in allen Teilen der Welt, so heben den Preis von 1800%.

Es ist erwähnenswert, dass etwa ein Drittel der Mittel der britischen Gesundheit angegriffen wurde im Mai mit dem HIV-Virus namens Loesegeldes (WannaCry), damit gedroht, entfernen Sie Tausende von Computern Daten, es sei denn ein Lösegeld balbtwkn entspricht etwa 230 Pfund für jedes Gerät. Aus diesem Grund store albtwkn aus Angst vor der Unternehmen zur Zahlung von Lösegeld.

Die Jahrzehnte albtwkn Aktien Futures in die Organisation einen Schritt in Richtung auf die Entwicklung solcher Währung digitale Kluft in der vorherrschenden Finanzsystem

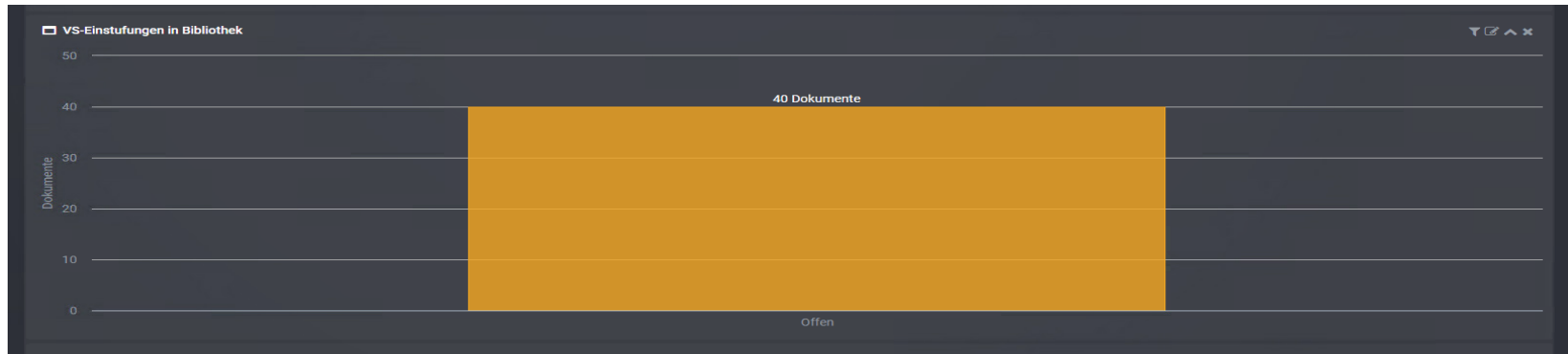
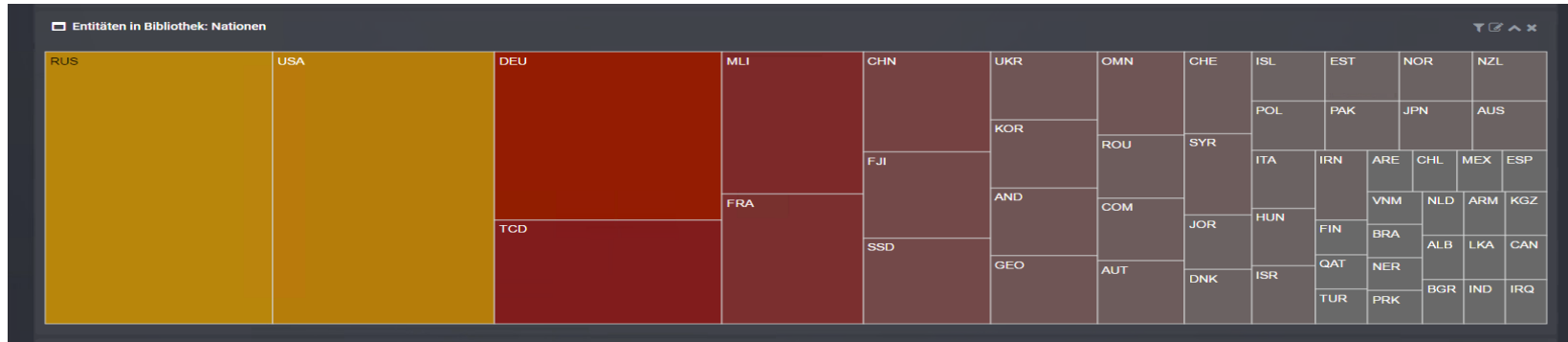
Es war geplant, um auf die TSE-albtwkn Futures-kontrakte in der CME-Unternehmen "Sonnenuntergang" gestern Nacht, eine Woche nach dem Start des "Global markyts kbw Rivalen" den Verkauf, die vom albtwkn.

Und Futures sind Finanzprodukte, mit denen die Händler die Wetten auf, ob der Preis von etwas nach oben oder unten über eine Zeit, in der Regel für die Verbreitung von Gold, Öl und andere Rohstoffe.

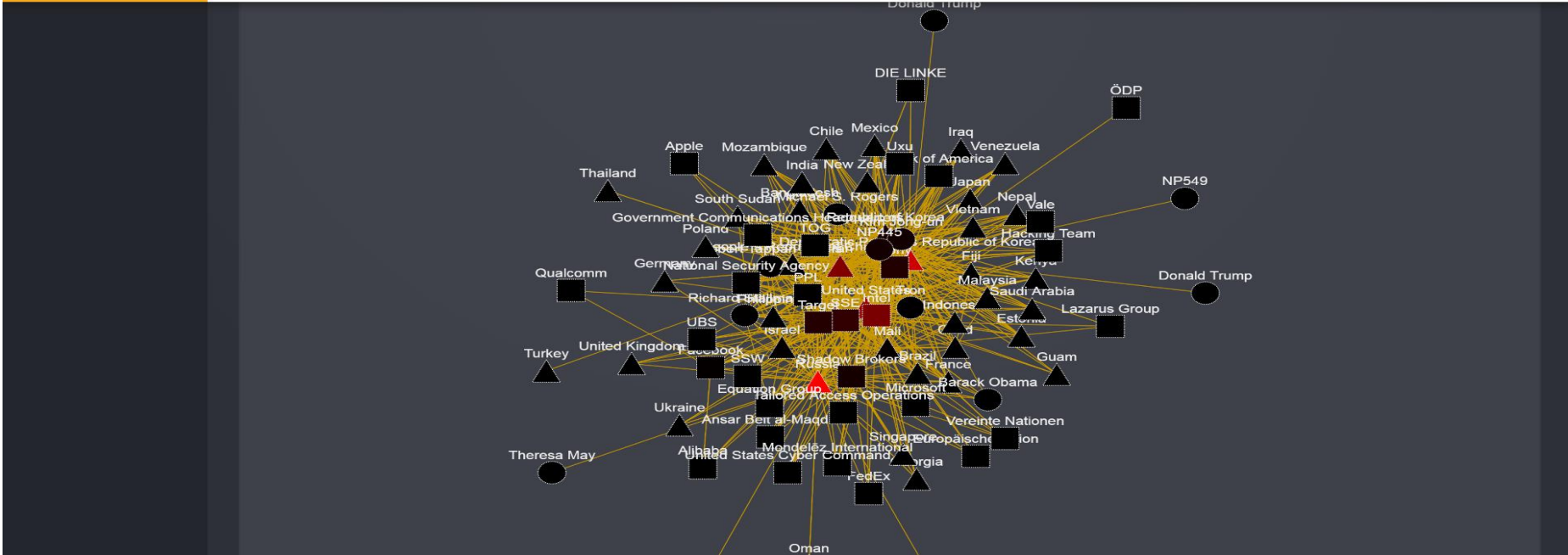
Start ist albtwkn Bestände Futures-kontrakte die Organisation einen Schritt in Richtung auf die Entwicklung der vorherrschenden albtwkn in das Finanzsystem und die Gründe für die hohen



# Analyse unstrukturierter Daten



# Analyse unstrukturierter Daten





# Analyse unstrukturierter Daten

## Export zu i2



20180219\_KdoCIR\_ANB\_Export\_Graph\_id\_76 (3) - IBM i2 Analyst's Notebook

Datei Home Anordnen Stile Analysieren Auswählen Ansicht Veröffentlichen

Einfügen Ausschneiden Kopieren Importieren Verbinden Verbundene Elementaktionen Quellen Zwischenablage Datenquellen Entitäten einfügen OLE-Objekt Textblock Kreis Ereignisrahmen Themenlinie Links einfügen Link Abknickung Aus Palette einfügen Paletten Benutzer Dynamisch Daten Karten Attribute Eigenschaften bearbeiten Löschen

20180219\_KdoCIR\_ANB\_Export\_Graph\_id\_76 (3) Diagramm2 Diagramm3

Analyse sozialer Netzwerke

Ergebnisse Optionen Gewichtungen

rbdbms-connector 101 im Diagramm

Berechnen: Betweenness

Offnen... Zuletzt verwendet

Ergebnisse vom Diagramm ausblenden  
Ergebnisse löschen  
Funf wichtigste auswählen  
Nicht ausgewählte ausblenden  
Alles anzeigen  
Elemente auflisten  
Ergebnistabelle kopieren

Ausgeblendete Elemente: Ohne Alles anzeigen

Übersichtsbereich An Fenster anpassen Auswahl an Fenster anpassen Originalgröße Diagramm ziehen



# Analyse unstrukturierter Daten

## Export zu i2



Diagramm2 - IBM i2 Analyst's Notebook

20180219\_KdoCIR\_ANB\_Export\_Graph\_id\_76 (3) Diagramm2 Diagramm3

Ergebnisse Optionen Gewichtungen

rdbms-connector 812 im Diagramm

Berechnen: Betweenness

Entität	Betweenne...
Tron	11.1330
Robert Tappan ...	9.3921
TOG	8.7292
Richard Stallman	8.4919
Kim Jong-un	7.9157
445	7.5471
Shadow Brokers	4.9892
Hacking Team	3.9370
Uxu	3.5178
United States	2.2913
Democratic Peo...	2.2913
Russia	1.7374
France	1.5094
Barack Obama	0.8715
Lazarus Group	0.7987
Equation Group	0.7160
Tailored Access ...	0.6347
Ukraine	0.3339
Michael S. Rogers	0.3226
People's Republ...	0.2894
Iran	0.2469

Ergebnisse im Diagramm anzeigen  
 Ergebnisse löschen  
 Fünf wichtigste auswählen  
 Nicht ausgewählte ausblenden  
 Alles anzeigen  
 Elemente auflisten  
 Ergebnistabelle kopieren





# Lagebericht CIR



