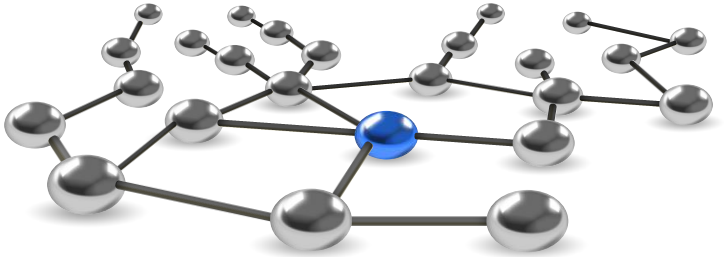
Internationaal forensisch datamanagement

Introductie FIM
Solution architectuur
Data integratie en data analyse
Integrated security implementatie

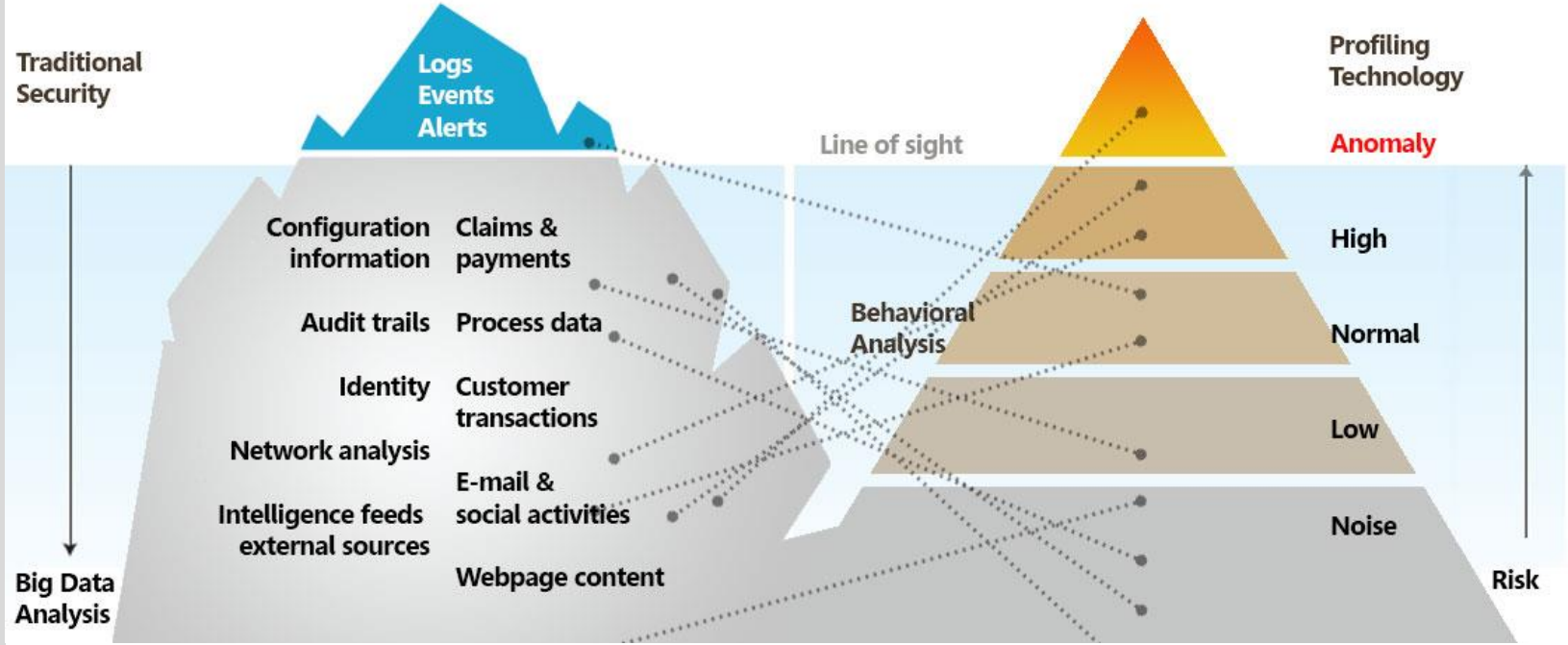
Innovators in financial crime risk

Forensic Incident Management?

- Het creëren van een 360 graden klantbeeld op **alle data** vanuit **alle locaties** om beter in staat te zijn financiële criminaliteit te detecteren, analyseren en uiteindelijk te voorkomen.



Van de top van de ijsberg tot de top van de pyramide

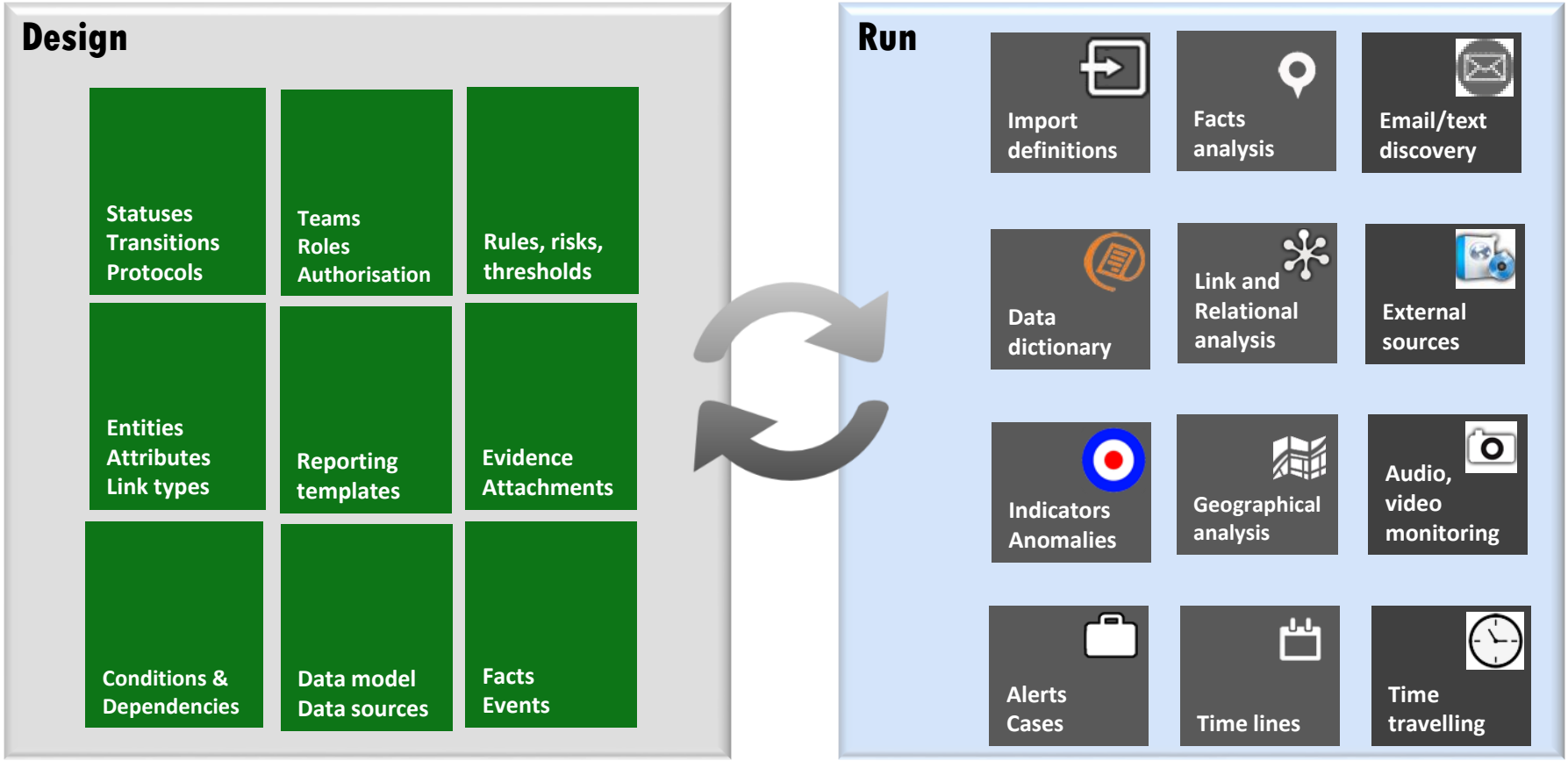


Een volledig geïntegreerd, aanpasbaar platform

Mensen, trades, organisatie, alerts, market data, zaken, historie, etc.

- gedragscontrole, interne en externe bronnen, met inbegrip van (forensisch) geschiedenis
- Complete onderzoek workflow processing, inclusief richtlijnen, protocollen & reports
- Stakeholder- and team management, delen van informatie en data gerelateerde samenwerking (en restricties)

Continue aanpasbare configuratie



Stelling

Omschrijving:
Er zijn 3 personen, ieder van hen is ook persoonlijk klant bij jou financiële organisatie.
Zij zijn samen eigenaar van dezelfde software start-up en zij komen als organisatie bij jou voor het aanvragen van een lening.

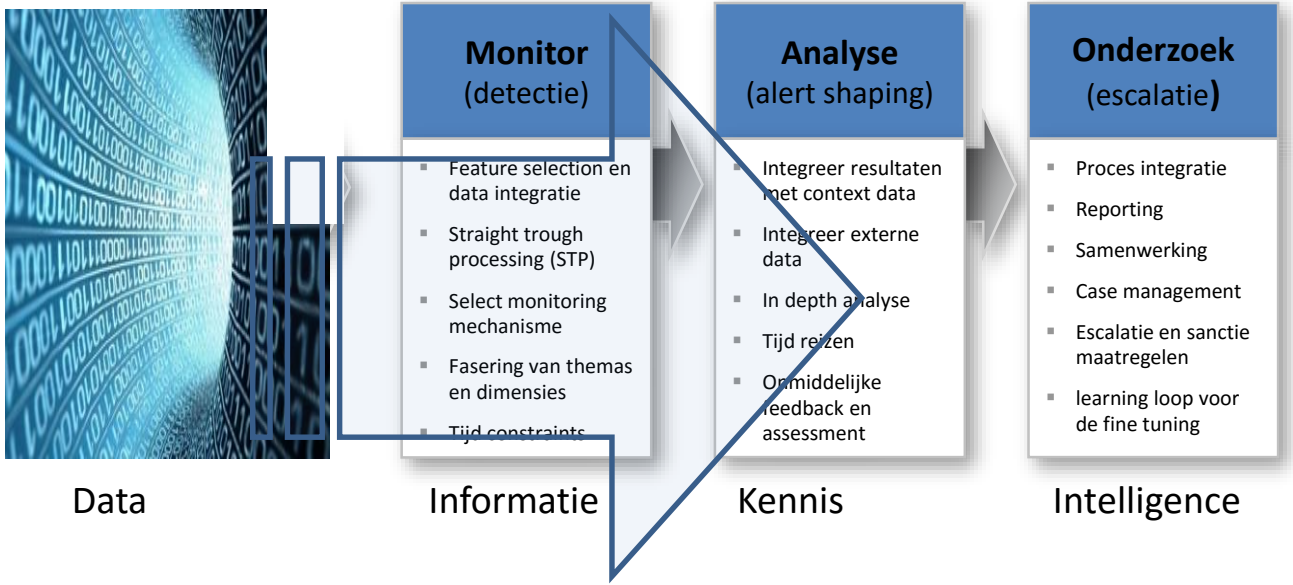
Zij hebben een volledig uitgewerkt Business Plan waarin zij uitleggen waarom hun software zo baanbrekend is, wat de potentie is, welke klanten zij al hebben en dat ze een patent hebben op hun software.

Vragen?
- Wat zou jij doen of wat heb jij nodig om het risico te onderzoeken?
- Zou jij op basis van bovenstaande informatie een lening overwegen?

Solution architectuur

De volgende slides beschrijven de gekozen processen en architectuur

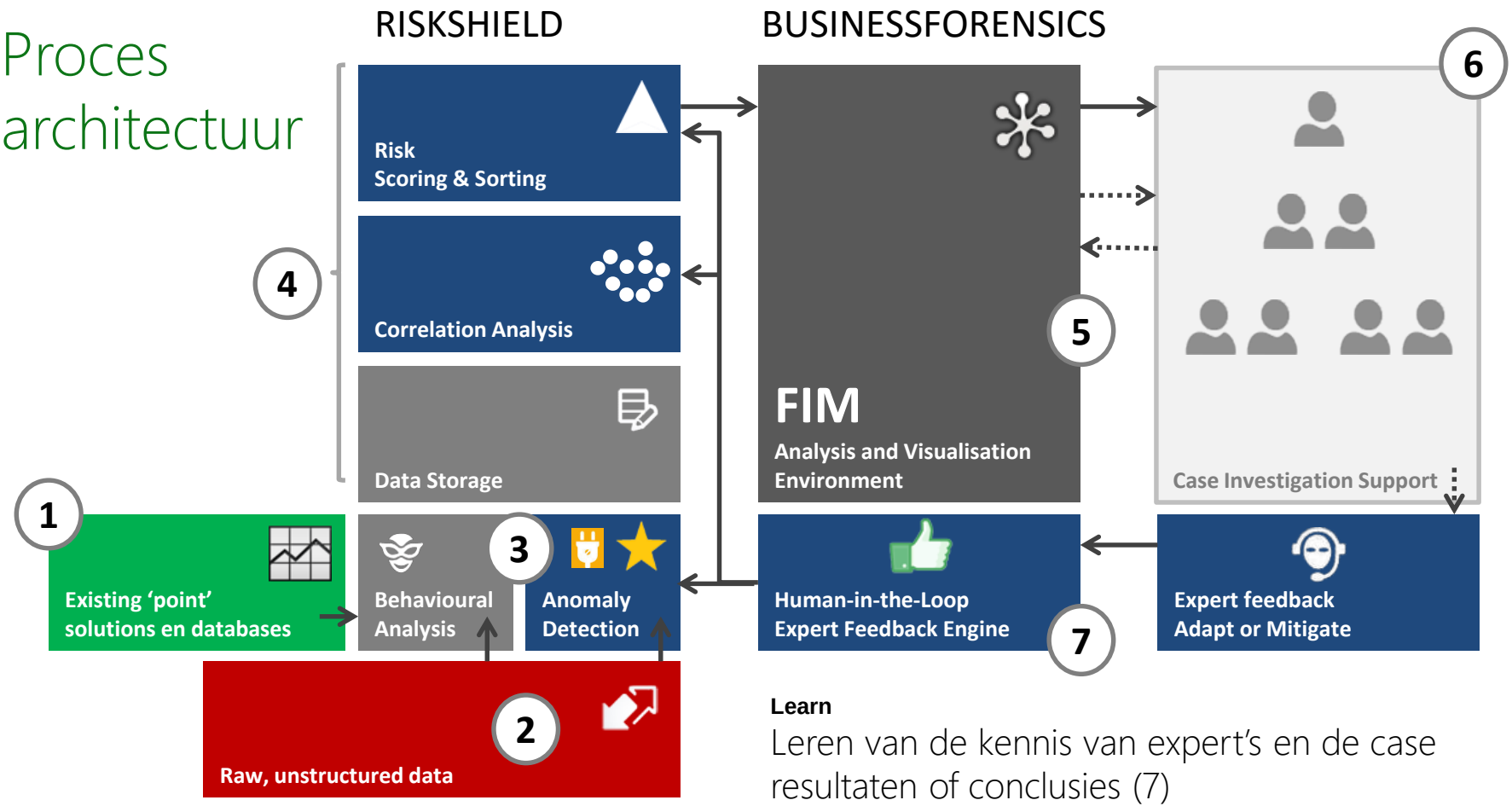
Van detectie naar analyse tot onderzoek



De belangrijkste uitgangspunten zijn naast het rangschikken van meldingen:

- Terugbrengen van het aantal “false postives”
- Vormen en prioriteren van alle alerts op een enkel platform
- Continue optimaliseren van detectie mechanisme

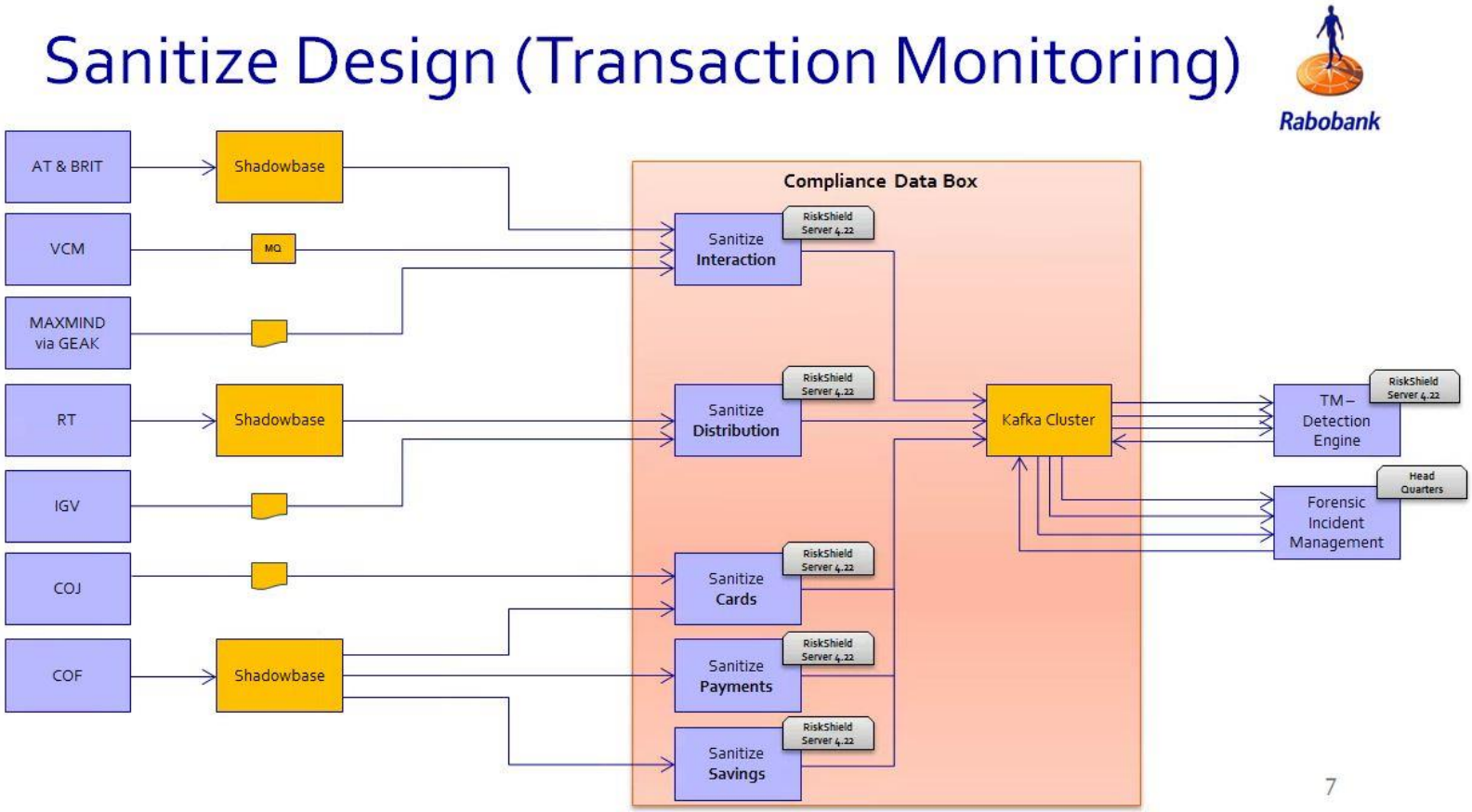
Proces architectuur



Learn

Leren van de kennis van expert's en de case resultaten of conclusies (7)

Voorbeeld data sanitizing en distributie



Data integratie en modeleren

De volgende slides beschrijven het forensisch data model en de manier waarop de verschillende data bronnen worden geïntegreerd

Dit data model is volledig configureerbaar en erg flexibel. Nieuwe data bronnen kunnen te alle tijde worden toegevoegd.

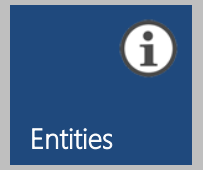
Forensic view on data

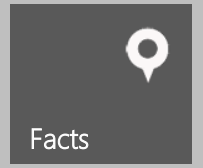
Internal: customers, contracts, accounts, etc.

External: registers, social media

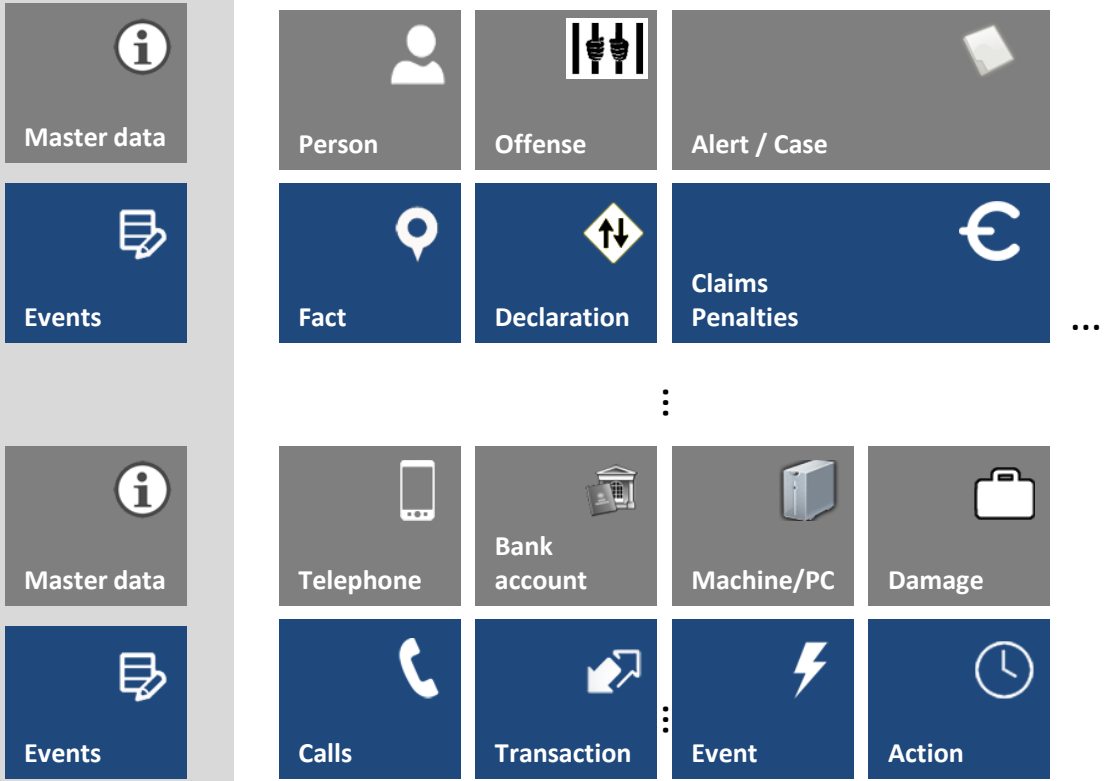
Watch lists, market data, collaborations

Events: transactions, trades, lending, log files





Van master data tot feiten (en vice versa)



Master data

- Unique geïdentificeerd
- Behoudt zijn informatieve waarde
- Links en attributen

Feiten

- Op een bepaalde tijd
- Verliest zijn informatieve waarde
- Features en dimensies

Stap 1

- Data analyseren
- Klant specifiek datamodel configureren

Stap 2

- Ruwe data importeren & extraheren
- Data opknippen in: entiteiten-attributen -feiten

Stap 3

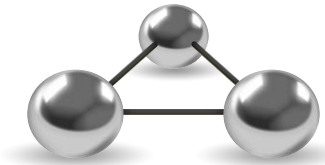
- Data samenvoegen
- Relaties definieren en identificeren

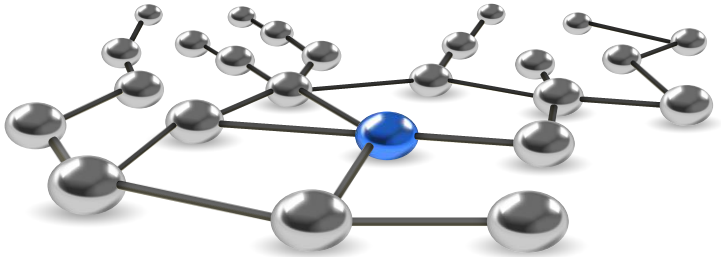
Stap 4

- Sociaal netwerk opbouwen
- Triage en data linken door harde en softe links

Stap 5

- Data verwerken
- Beschikbaar voor alle modules
- 360° klantbeeld

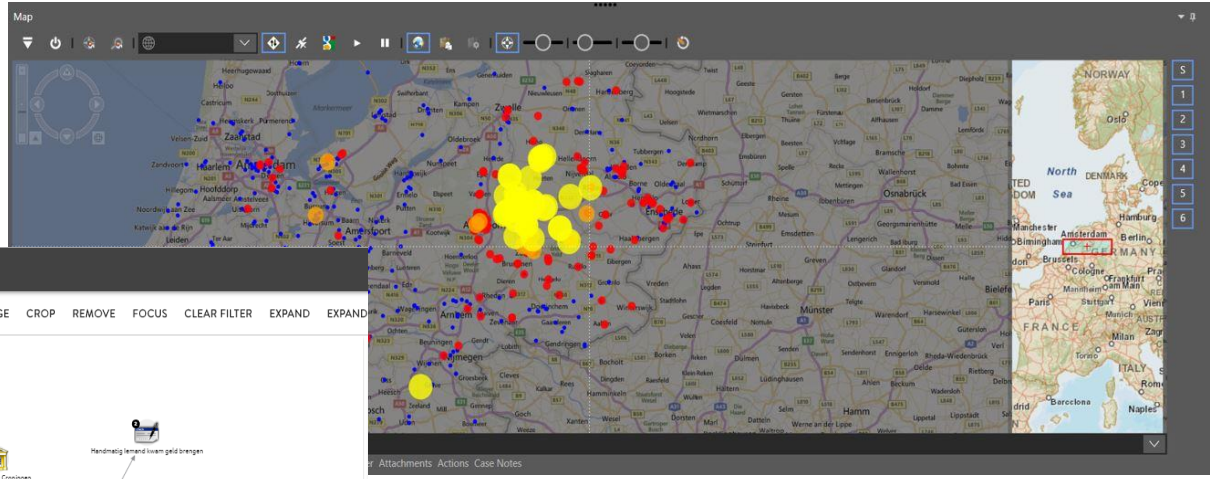




Alle data formaten & kwaliteiten
Alle beschikbare bronsystemen
Transacties & non-transactionele data

'Opgeknipt' in:
Objecten, attributen, feiten & relaties

En weer aan elkaar gelinkt op verschillende manieren:
360° risk view op basis van alle data


Map
NORWAY
Oslo
North Sea
DENMARK
Amsterdam
Hamburg
Berlin
Brussels
Paris
FRANCE
Milan
Barcelona
Naples
Attachments
Actions
Case Notes

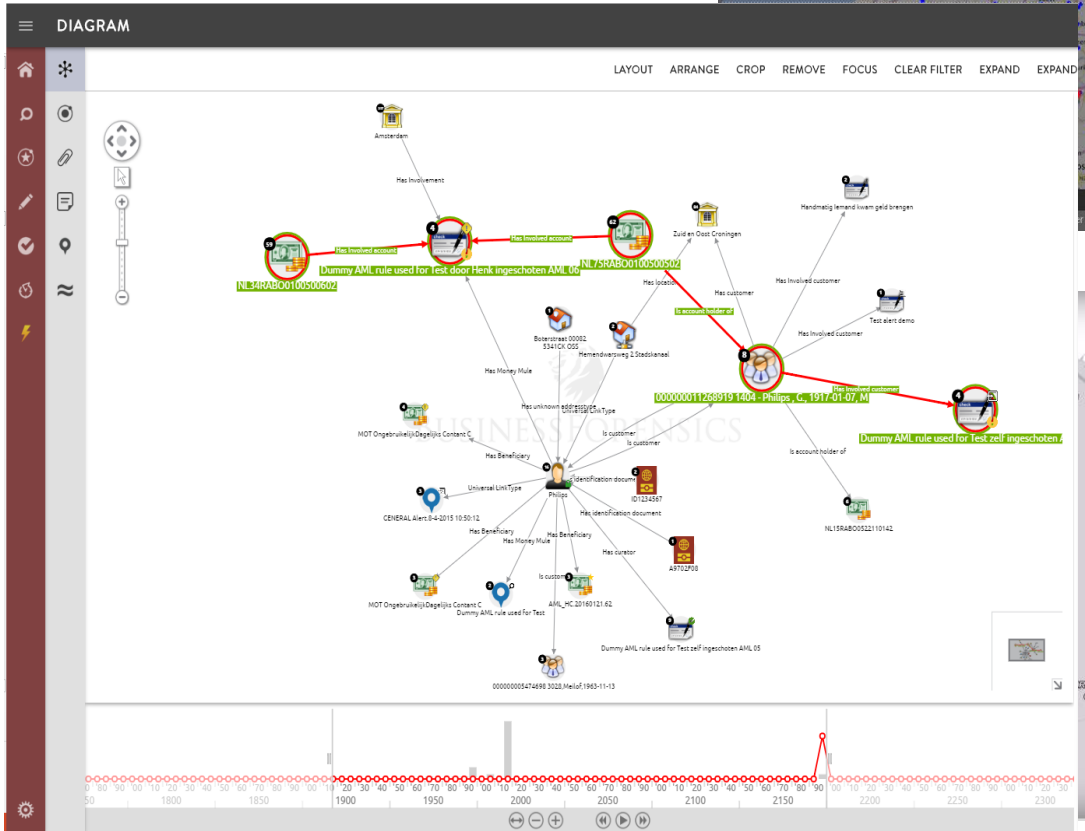


DIAGRAM
LAYOUT
ARRANGE
CROP
REMOVE
FOCUS
CLEAR FILTER
EXPAND
EXPAND
Amsterdam
Has Involvement
Has involved account
Has involved account
Dummy AML rule used for Test door Henk ingeschoten AML 06
NL34RABO0100500502
NL75RABO0100500502
Zuid en Oost Croningen
Has location
Has customer
Is account holder of
Handmatig iemand kwam geld brengen
Has involved customer
Test alert demo
Has involved customer
Has Money Mule
Has unknown addressType
Universal LinkType
0000000011268919 1404 - Philips , C., 1917-01-07, M
Has involved customer
Dummy AML rule used for Test zelf ingeschoten A
MOT Ongebruikelijk Dagelijks Contanc C
Is customer
Is customer
Is account holder of
Has Beneficiary
Identification docume
Philips
ID1234567
Universal LinkType
CENERAL Alert 9-4-2015 10:50:12
Has identification document
Has Beneficiary
Has Money Mule
Has Beneficiary
Has curator
A9702F08
NL15RABO0522110142
MOT Ongebruikelijk Dagelijks Contanc C
Dummy AML rule used for Test
Is customer
AML_HC_20160121.62
Dummy AML rule used for Test zelf ingeschoten AML 05
0000000054749B 3028.MeloF.1963-11-13


Canada
Vancouver
Montréal
Toronto
Los Angeles
Mexico
Mexico City
Havana
Cuba
Haiti
Dominican Republic
Puerto Rico
Jamaica
Belize
Honduras
El Salvador
Caracas
Chart Mode:
Map Mode
Network Mode
Show routes in foreground on hover
Show routes with more flights than: 2500
AA American
AS Alaska
B6 JetBlue
DL Delta
EV ExpressJet
F9 Frontier
FL AirTran
HA Hawaiian
MQ Envoy
OO SkyWest
UA United
US US Airways
VX Virgin
WN Southwest
All
Clear
Invert

Integrated Security Implementatie

De volgende slides beschrijven de autorisatie structuur die wij inzetten om de data beschikbaar en visueel te maken over de verschillende teams, landen en service consumers heen.

Autorisatie infrastructuur (1)

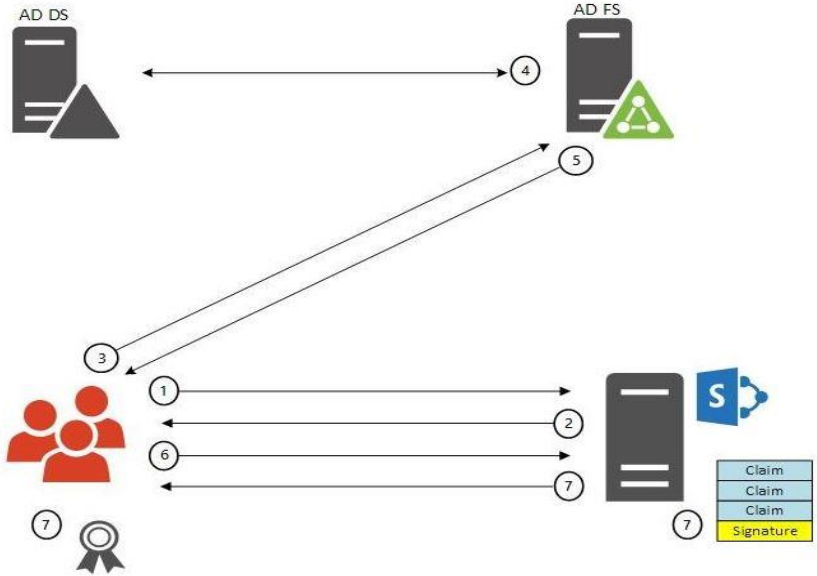
- Binnen onze autorisatie structuur hebben wij de beveiliging van de data volledig overgedragen aan het Windows Operating System en de Active Directory/ADFS in het bijzonder.

- De reden hiervoor is dat wij een forensische database hebben waarbij bijv. de entiteiten tabel ALLE objecten bevat waarmee het systeem werkt, of het nu gaat om een voertuig, organisatie, document of ander ‘ding’. Hierdoor moet een gebruiker specifiek rechten kunnen krijgen op een object.

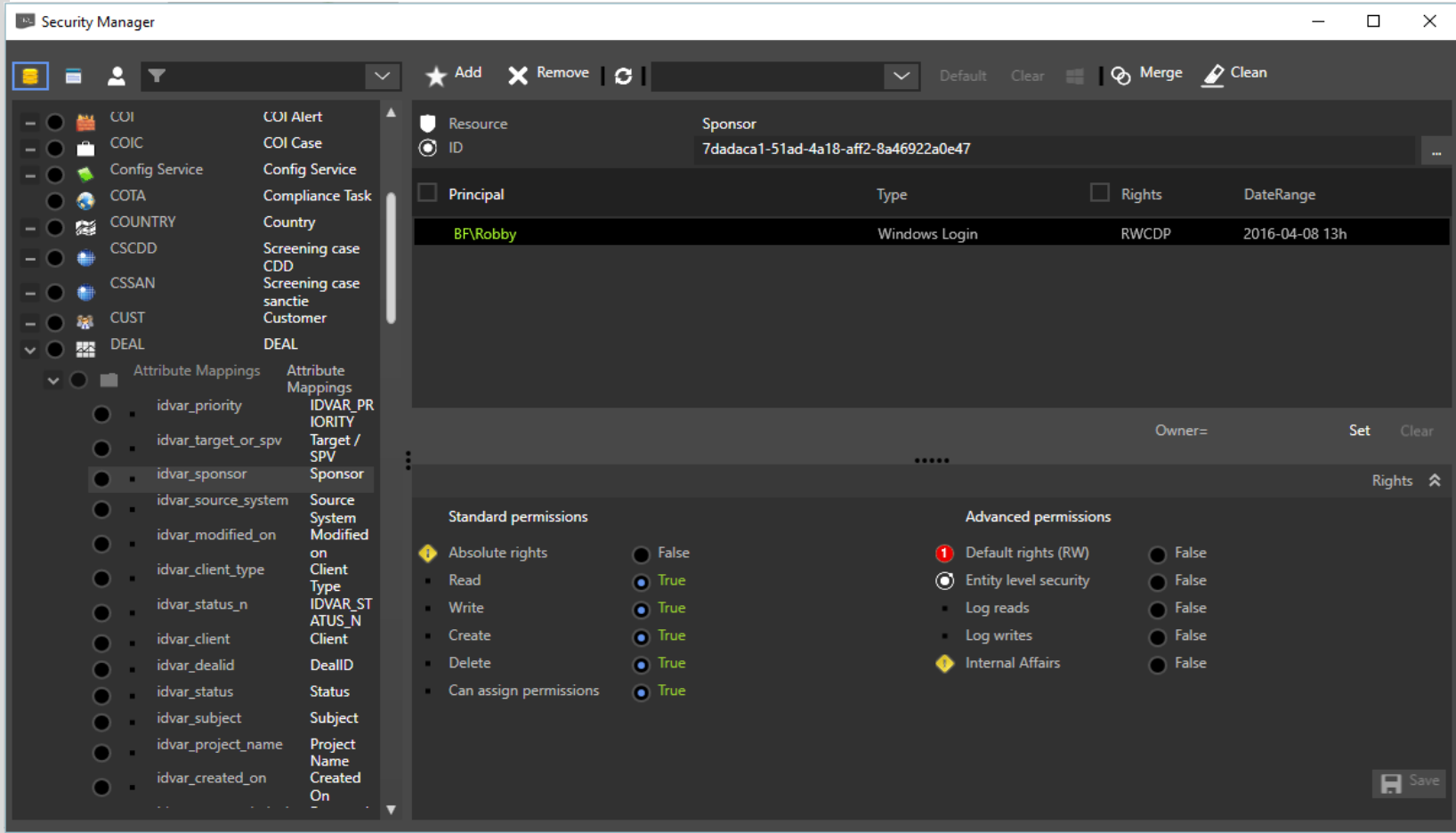
Autorisatie infrastructuur (2)

DUAL TOKEN Autorisatie

1. Gebruiker opent de web-applicatie.
2. Applicatie stuurt de gebruiker naar de identity provider om security token.
3. De identity provider vraagt de gebruiker om zijn credentials.
4. De identity provider valideert de credentials met de authenticatie provider (ADFS).
5. Als het succesvol is krijgt de gebruiker een security token.
6. De identity provider stuurt de gebruiker een SAML security token.
7. De gebruiker stuurt een nieuw request naar de web-applicatie met het SAML token.



Autorisatie op data niveau



Autorisatie op functioneel niveau