



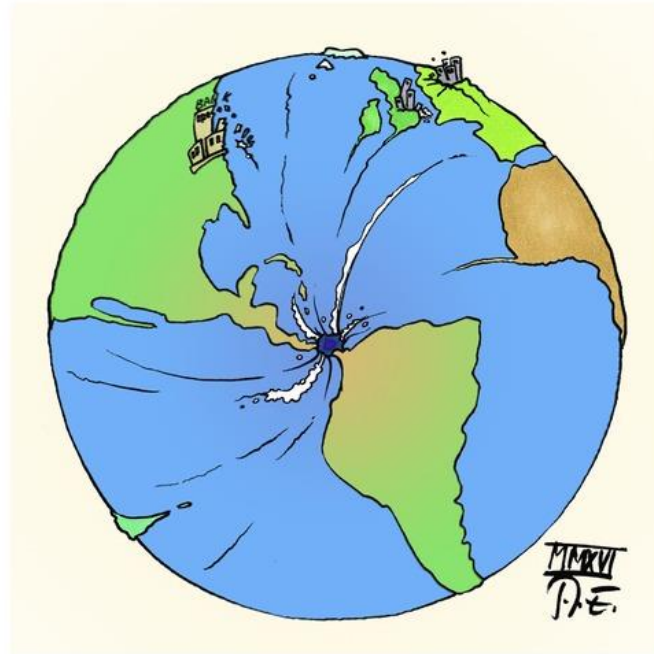
SIRA - Minder waar het kan, meer waar het moet

02.06.2016



Onno de Vrij
SAS Institute

Integriteitsproblemen leiden tot ...



... reputatieschade.



Integer of niet?

Er is geen duidelijke grens

- Wielerteams die onderling afspraken maken in de Giro
- Plug-In Hybride auto's met lage bijtelling
- Congres bezoek in Zuid-Afrika
- Groene beleggingen
- 128 km/h uur rijden waar het 120 km/h is
- Uit eten met een klant
- Fles wijn met kerst
-

Een definitie van integriteit

Integriteit houdt in:

- Zeggen wat u doet en doen wat u zegt;
- Uzelf aan principes en overtuigingen houden;
- Consequent handelen naar uw eigen normen en waarden;
- Uzelf ook onder druk aan uw afspraken houden;
- Uzelf en anderen [vertrouwen](#) tot het tegendeel is gebleken;
- Niet omkoopbaar zijn of uit eigenbelang van uw principes afwijken;
- Vrijmoedig spreken en voor uw mening uitkomen waar dat **nodig** en **mogelijk** is;
- Een besef van gezonde eigenwaarde hebben. *(Dit is iets anders is dan eigenbelang).*

Bron: Heinpragt.com

A close-up photograph of the bottom of a red plastic bottle cap. The cap is held by a person's fingers, visible at the top and bottom edges. The bottom surface of the cap is white and features a circular yellow label. On the label, the text "integrity is doing the right thing when no one is watching" is printed in a black, sans-serif font, arranged in five lines. The background is a blurred, dark grey surface.

integrity
is doing the
right thing when
no one is
watching

Wat vraagt DNB van ons?

Systematische Integriteit Risico Analyse

SIRA

De integriteit-
risicoanalyse

Meer waar dat
moet, minder
waar dat kan

DeNederlandscheBank

EUROSYSTEEM

Nog een stuk wetgeving erbij?



Voorbeelden van integriteitrisico's

- Witwassen
- Terrorismedfinanciering
- Omzeiling sanctieregelgeving
- Corruptie (omkoping)
- Belangenverstrengeling
- Interne en externe fraude
- Ontduiking of ontwijking van fiscale regelgeving
- Marktmanipulatie
- Cybercrime
- Maatschappelijk onbetamelijk gedrag

Bezint eer ge begint



SIRA in 2015 - Opzet

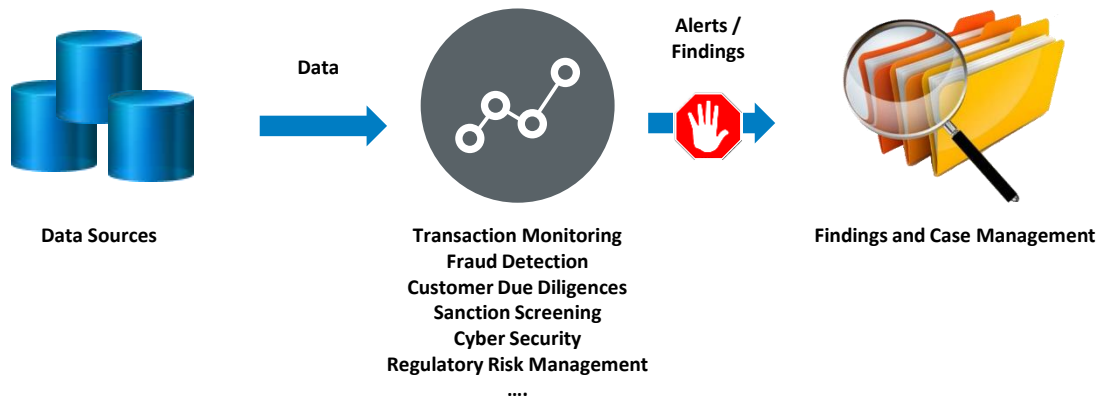
1. Een duidelijke organisatieschets
2. Relevante **risicoscenario's**
3. Doordacht scoringssysteem
4. Eerlijke beoordeling effectiviteit beheersing
5. Risico's afgezet tegen **risk appetite**
6. Netto risico's en **gaps**
7. **Sturingsdocument** voor management
8. **Communicatie** binnen instelling

SIRA in 2016 - Werking

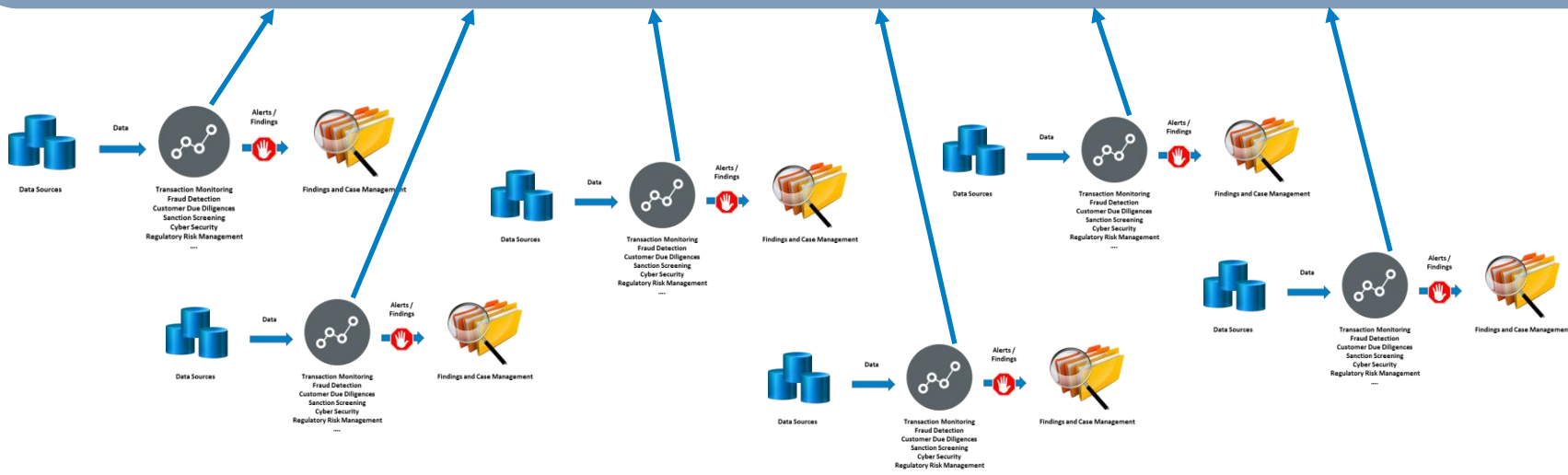
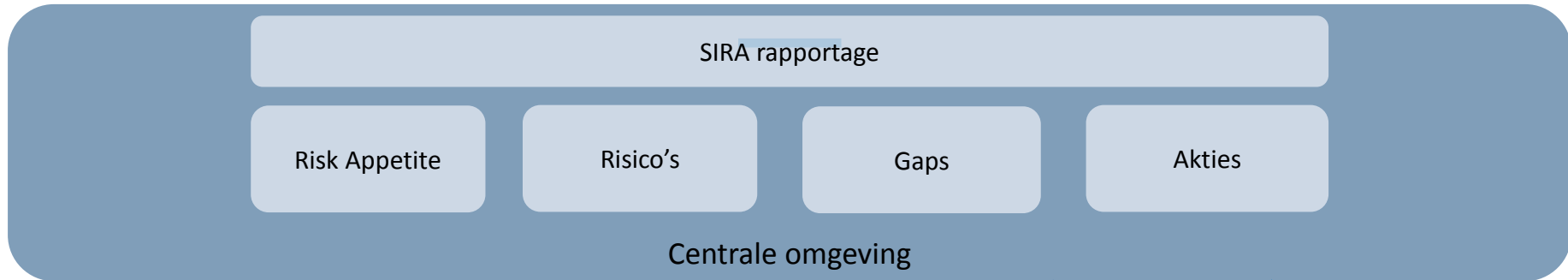
1. Passen bruto en netto risico's binnen de risk appetite?
2. Gebruik van de uitkomsten van de analyse?
3. Hoe worden geïdentificeerde gaps opgepakt?

Hoe kunnen we dit aanpakken?

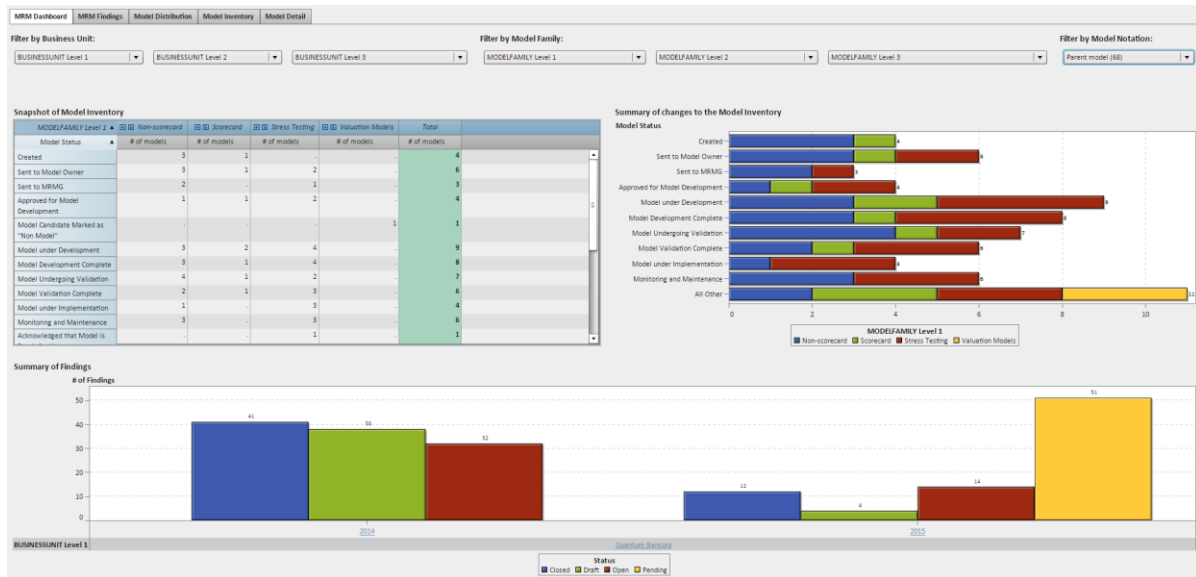
Uitkomsten van onze systemen ...



...rollen op naar een centrale omgeving ...



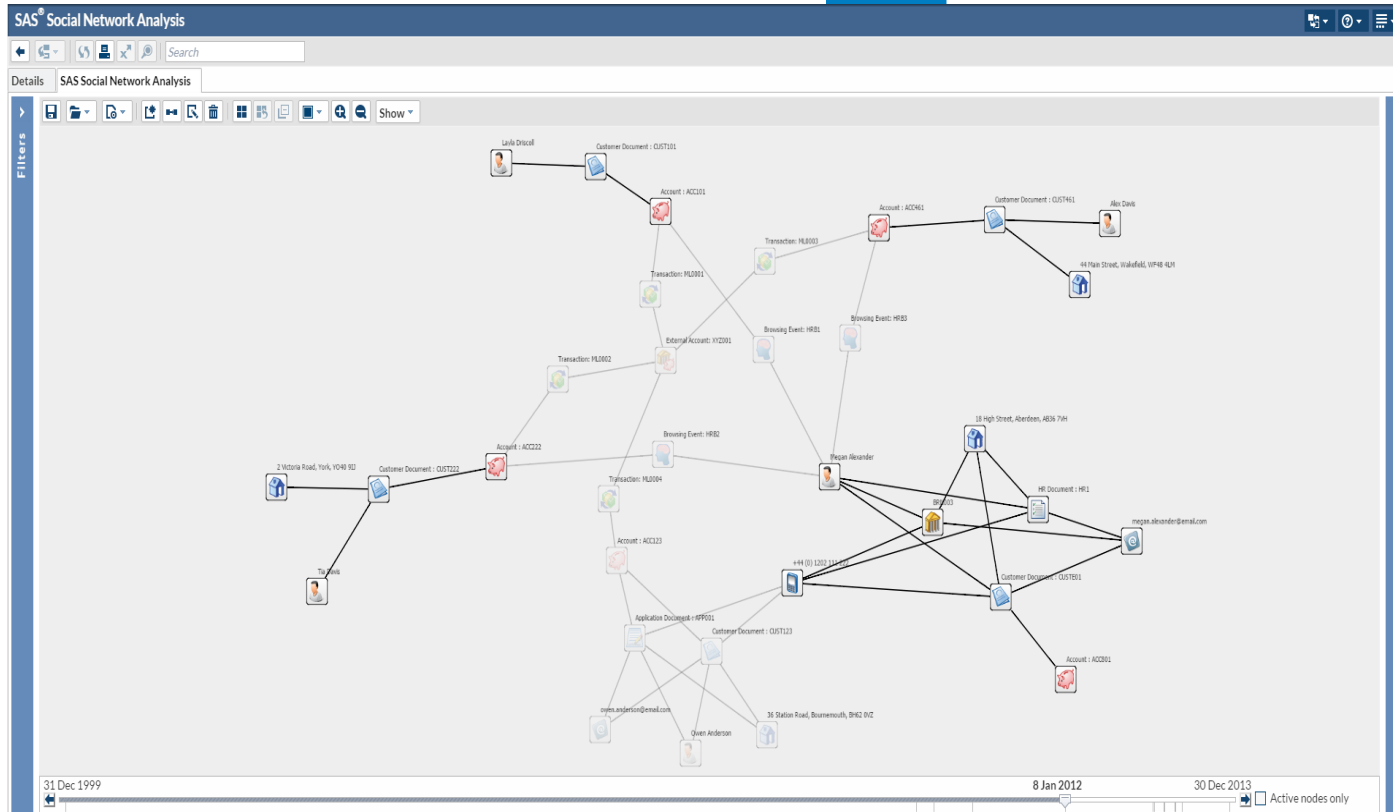
... voor risico identificatie, akties en rapportage.



Ken je je eigen medewerkers?

Interne Fraude

Het interne netwerk



	Individual
	Address
	Mobile Number
	Transaction
	Application
	External Account
	Internal Account
	Branch
	HR document
	Account Browsing
	Email Address
	Customer Document

Ken je je klanten?

CDD – UBO – AML

CDD – UBO – AML

Het proces

Data
Integration
and Lineage

Entity
Resolution

Extensive
matching
techniques

Quality
Knowledge
Base (QKB)

Extendable
Data Model

Data Prep

Entity Resolution

Disparate data sources



John Smith 13/01/1980 18 Queen Street JN 12 34 56 A



John Smith 13/01/1980



J. Smith 13/01/1980 18 Queen Street 0208 123 45676



John Smythe JN 12 34 56 A



Smith 13/01/1980 0208 123 45676

Data Prep

Entity Resolution



John Smith	13/01/1980	18 Queen Street	JN 12 34 56 A	
John Smith	13/01/1980			
John Smith	13/01/1980	18 Queen Street		0208 123 45676
John Smythe			JN 12 34 56 A	
Smith	13/01/1980			0208 123 45676

CDD / AML

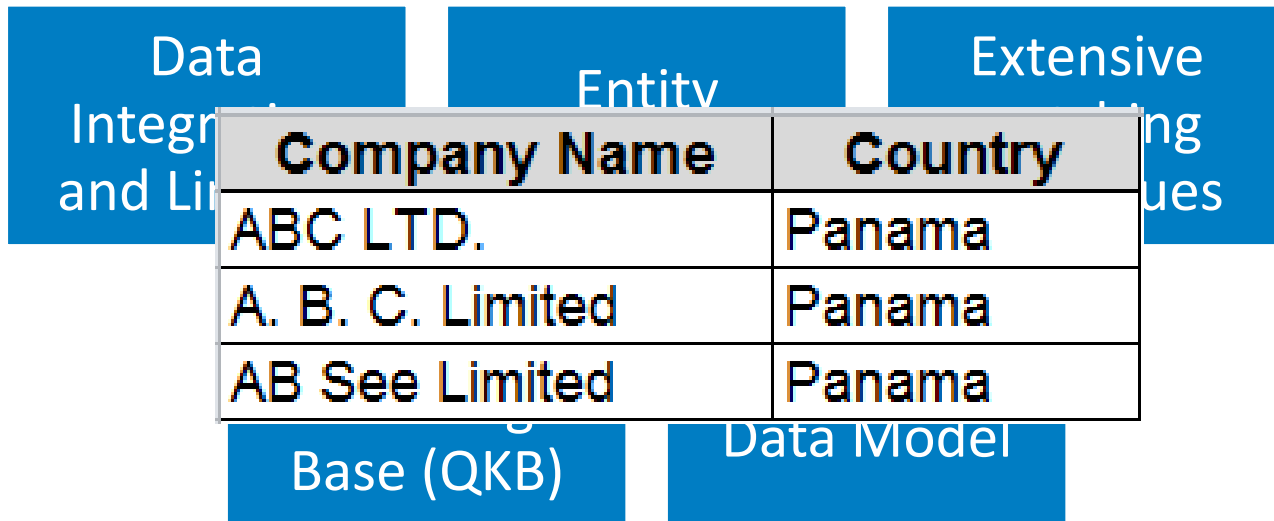
Entity Resolution



John Smith	13/01/1980	18 Queen Street	JN 12 34 56 A
John Smith	13/01/1980		
J. Smith	13/01/1980	18 Queen Street	0208 123 45676
John Smythe			JN 12 34 56 A
Smith	13/01/1980		0208 123 45676

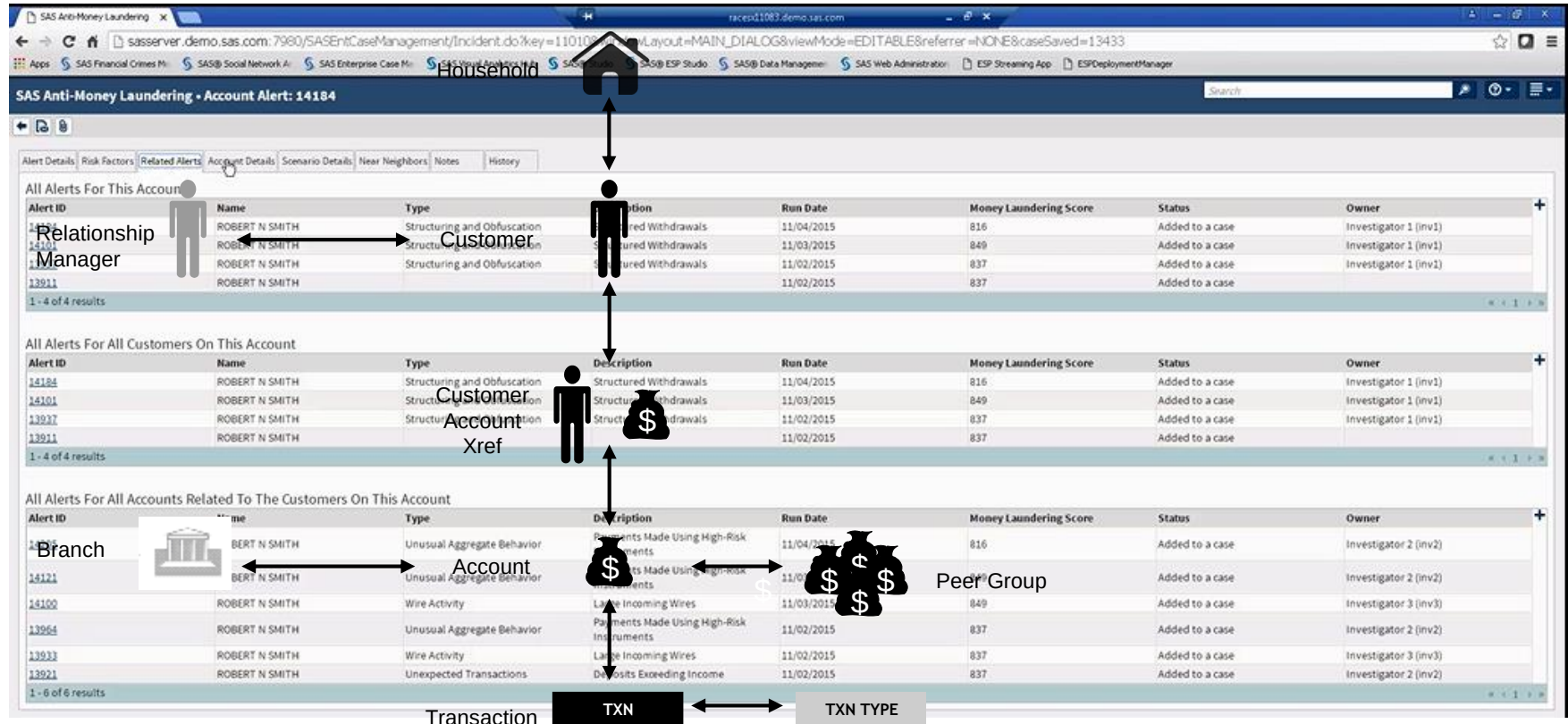
CDD – UBO – AML

Het proces



Data Prep

Core Dimensional Data Model



Houd je de foute mensen buiten?

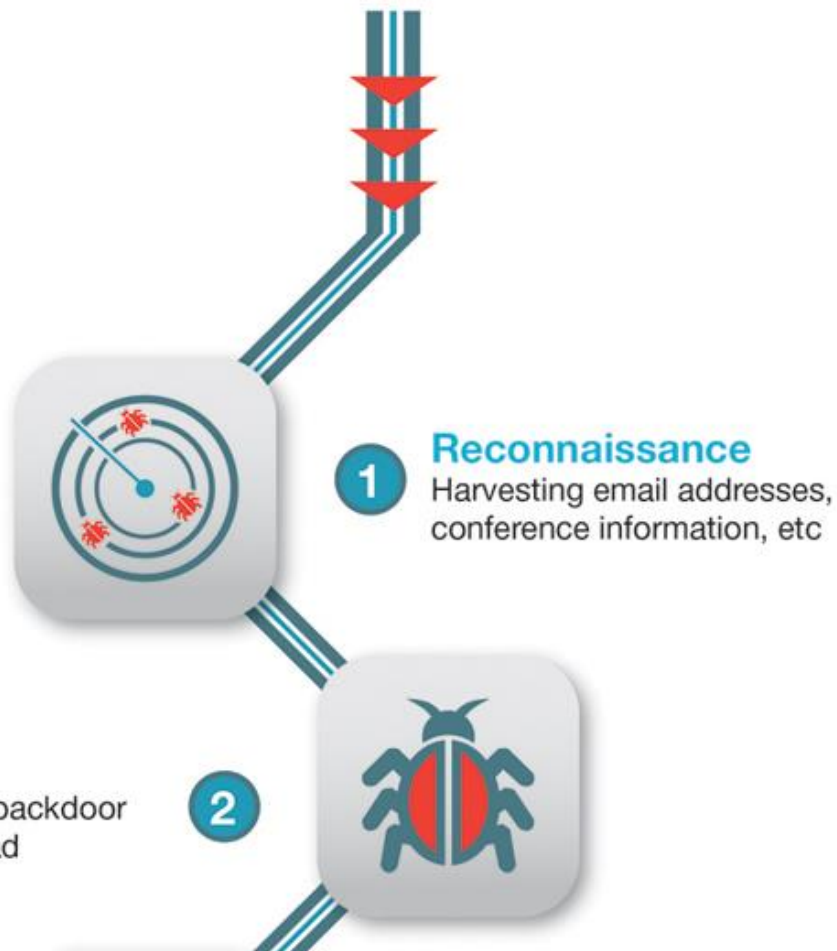
Cyber Security

Cyber Kill Chain®



Timeline

Hours to Months



1

Reconnaissance

Harvesting email addresses, conference information, etc

2

Weaponization

Coupling exploit with backdoor into deliverable payload

Preparation

Hours

Seconds

Weaponization

Coupling exploit with backdoor into deliverable payload

2



3

Delivery

Delivering Weaponized bundle to the victim via email, web, usb etc.



4

Exploitation

Exploiting a vulnerability to execute code on victim's system



5

Installation

Installing malware on the asset



Intrusion

Months



5

Installation

Installing malware on the asset

Command & Control (C2)

Command channel for remote manipulation of victim's system

6



7

Action on Objectives

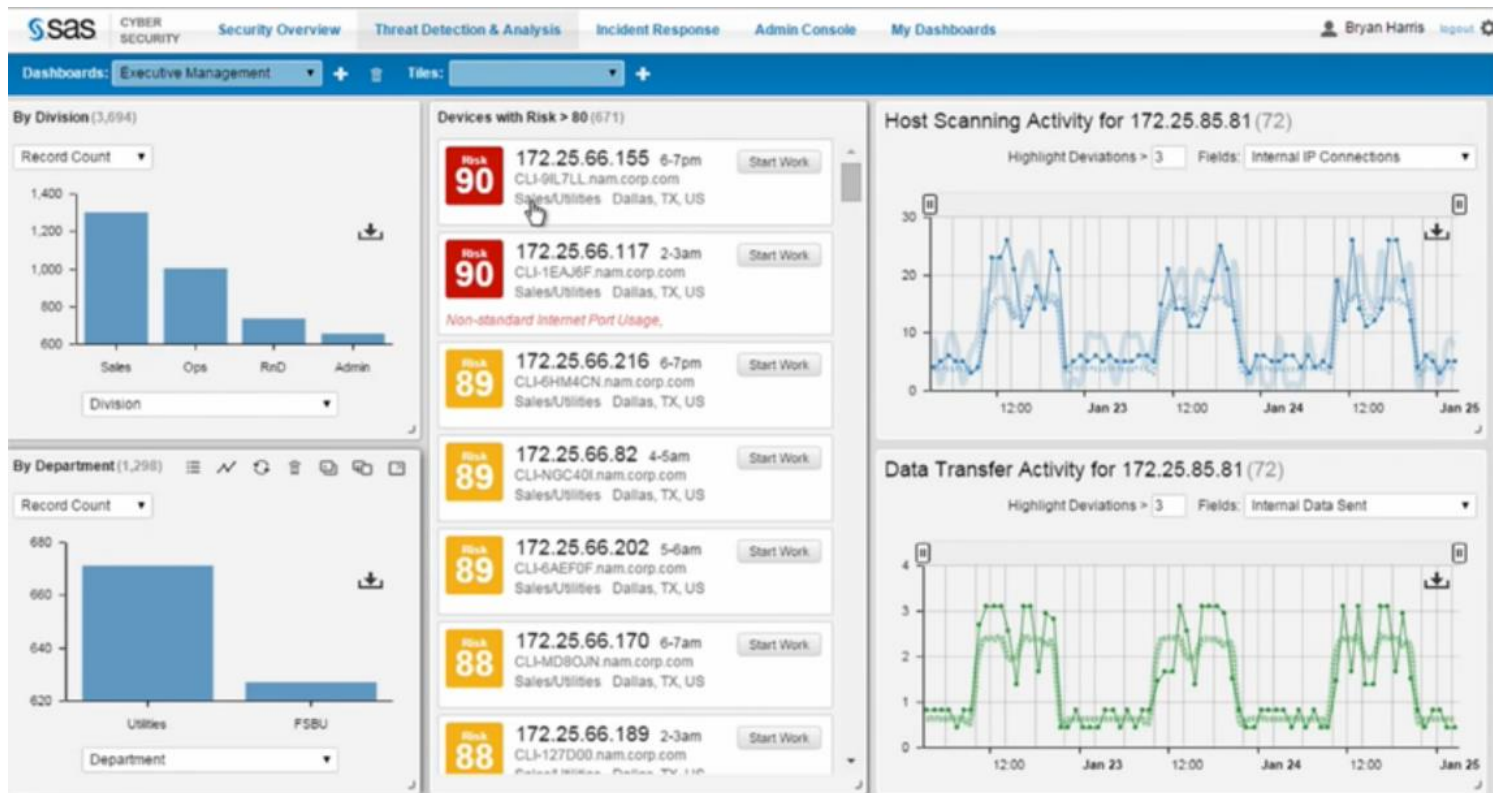
With 'Hands on Keyboard' access, intruders accomplish

Based on Lockheed Martin's Cyber Kill Chain

Active Breach

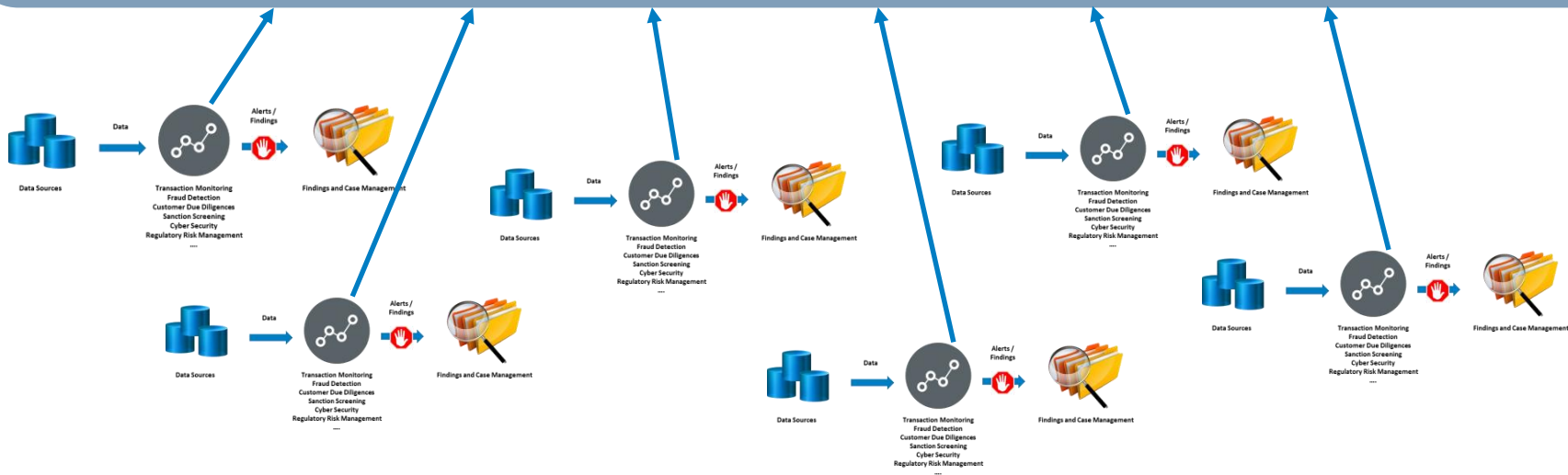
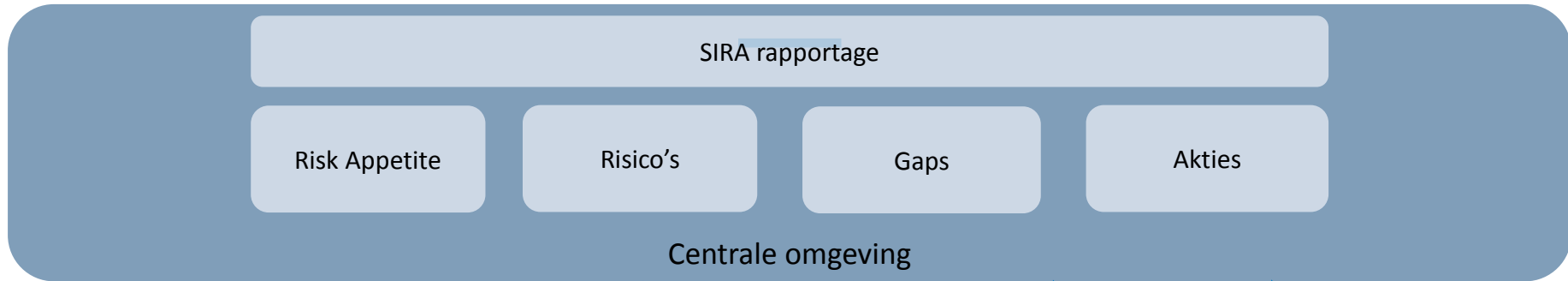
SAS for Cyber

Real Time Behavioral Network Analytics



Korte recap

Het SIRA proces



Hoe nu verder?

Systematische integriteitsrisicoanalyse nog niet overal in orde

Nieuwsbericht DNB van 30 mei 2016

DNB - 30 mei 2016

Vorig jaar deed DNB uitgebreid onderzoek naar de opzet van systematische integriteitsrisicoanalyses (SIRA's) van financiële instellingen. Daaruit bleek dat de meeste financiële instellingen hun SIRA niet op orde hebben. Daarom besloot DNB tot vervolgonderzoek in 2016.

Positieve ontwikkeling maar nog veel te doen

De afgelopen maanden beoordeelde DNB de SIRA's van vijftig instellingen, evenredig verdeeld over vijf sectoren: banken, betaalinstituten, pensioenfondsen, verzekeraars en trustkantoren. De eerste resultaten laten een wisselend beeld zien. Positief is dat het **merendeel** van de onderzochte financiële instellingen de **SIRA inmiddels op orde** blijkt te hebben. Diverse instellingen hebben substantiële vooruitgang geboekt. Maar **een aantal financiële instellingen** beschikt **nog niet** over een adequate SIRA. Dit is teleurstellend, vooral ook in ogenschouw genomen de uitgebreide informatievoorziening waarin DNB in 2015 heeft voorzien (zoals de publicatie van de brochure 'De integriteitsrisicoanalyse, meer waar dat moet, minder waar dat kan' en het organiseren van seminars).

Terugkoppeling

Alle onderzochte financiële instellingen krijgen een terugkoppeling in de komende periode. Ook gaat DNB na welke **toezichtmaatregelen** nodig zijn voor de financiële instellingen met een ondermaatse SIRA.

Nader onderzoek naar werking van de SIRA

Later dit jaar doet DNB onderzoek naar de beheersing van de integriteitsrisico's. In dit themaonderzoek wordt gekeken naar de **werking van de SIRA**, de toetsing van de uitkomsten hiervan aan de risk appetite van de financiële instelling en de vraag of de door de financiële instelling gehanteerde procedures en maatregelen goed zijn afgestemd op de gesignaleerde risico's. Indien uw financiële instelling wordt geselecteerd voor dit onderzoek, krijgt u daarover later bericht.

SIRA is niet het einde

Het is de basis voor een integere organisatie



Bedankt voor uw aandacht

Onno.de.Vrij@sas.com