Secuirty Scientist

ba@h2o.ai

H₂O
WORLD
2 0 1 7

Anomalous Behavioural Algorithms
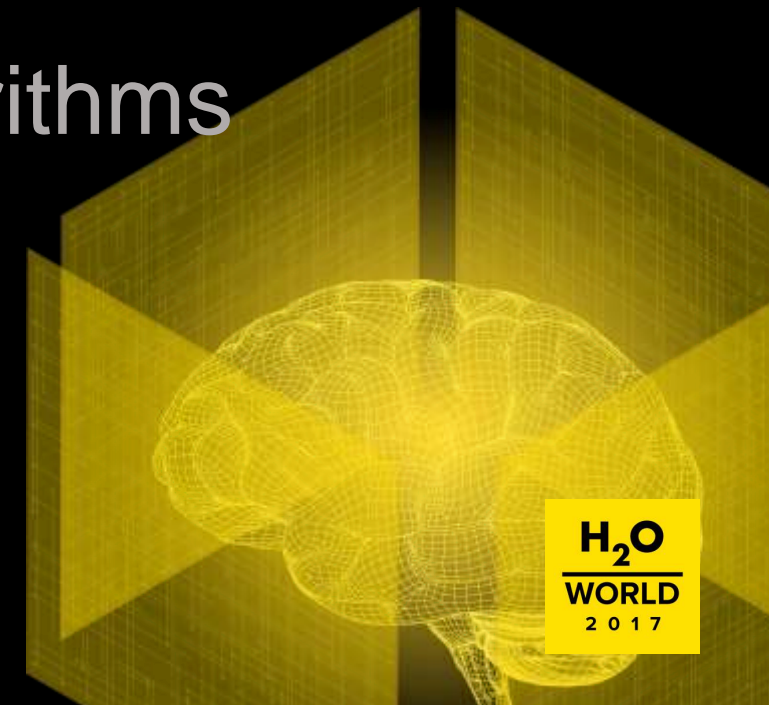
What is Money Laundering?

Breakdown

PLACEMENT

Collection of Dirty Money

Dirty Money Integrates into the Financial System

A TYPICAL MONEY LAUNDERING SCHEME

LAYERING

Payment by "Y" of False Invoice to Company "X"

Transfer on the Bank Account of Company "X"

Loan to company "Y"

Wire Tranfers

Offshore Bank

Purchase of Luxury Assets
Financial Investments
Commercial/Industrial Investments

INTEGRATION

iHazInfos.com

- Source: Ihazinfos.com

H₂O WORLD 2017

Sources of Illegal Money

Unrecorded Sources of Income

Human Trafficking

Source: anandnimesh.com, texasrightolife.com, newsofthesouth.com.

H₂O WORLD 2017

How does it affect us (society) ?
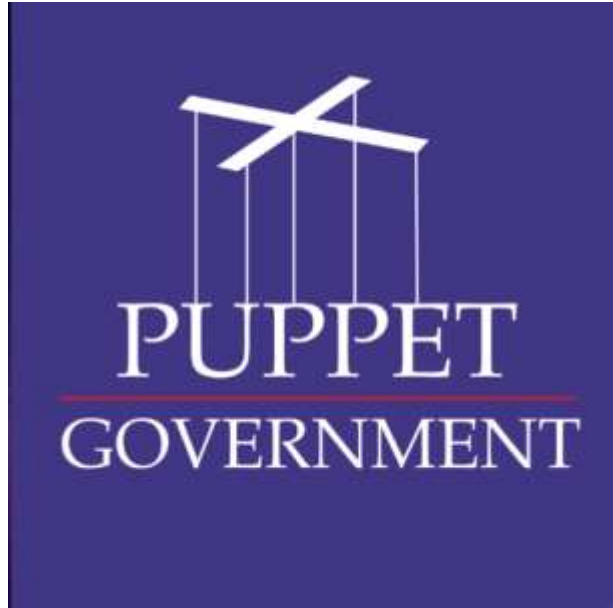
How do we catch it now?

Security Analyst

AML Alerts generated by rule systems. → Alerts → **True Positive Cases** / **False Positive Cases**
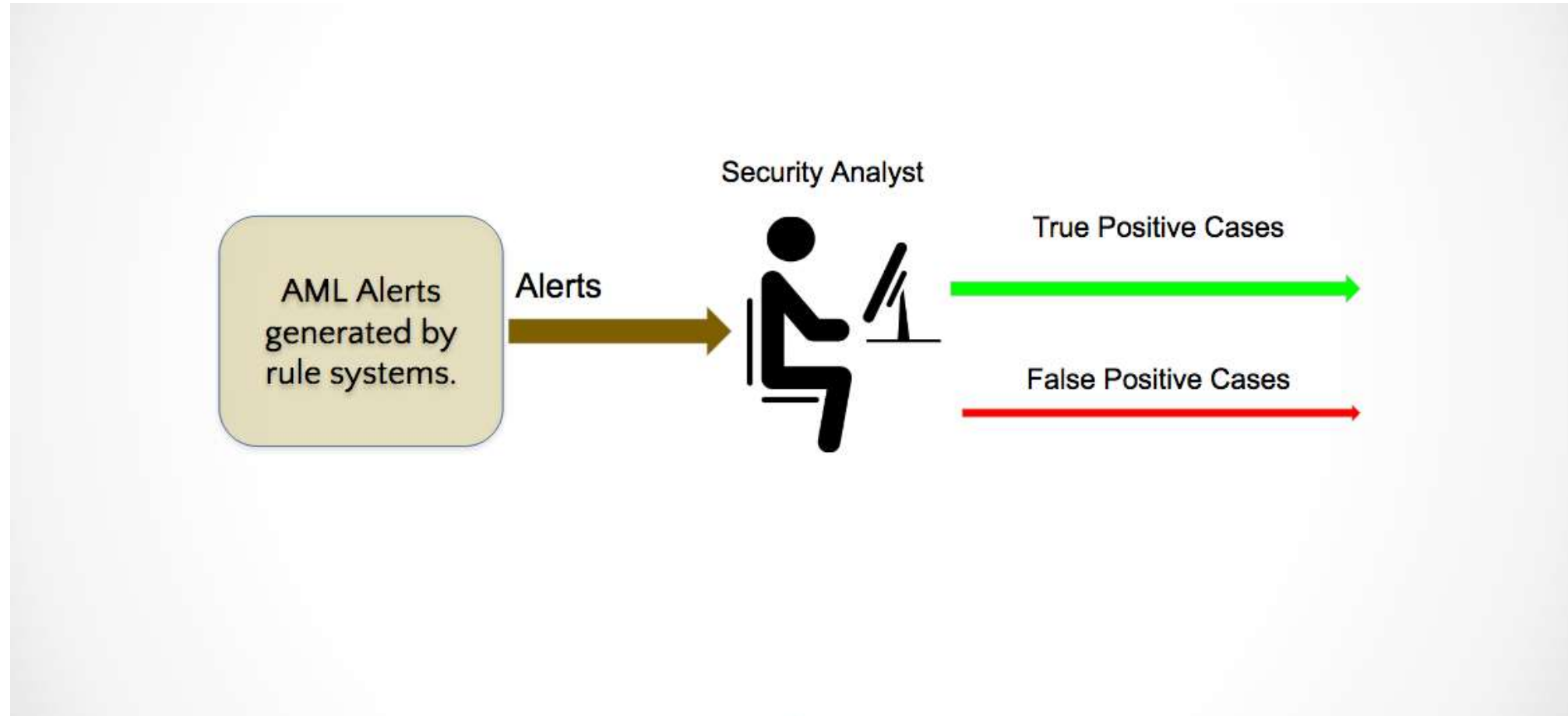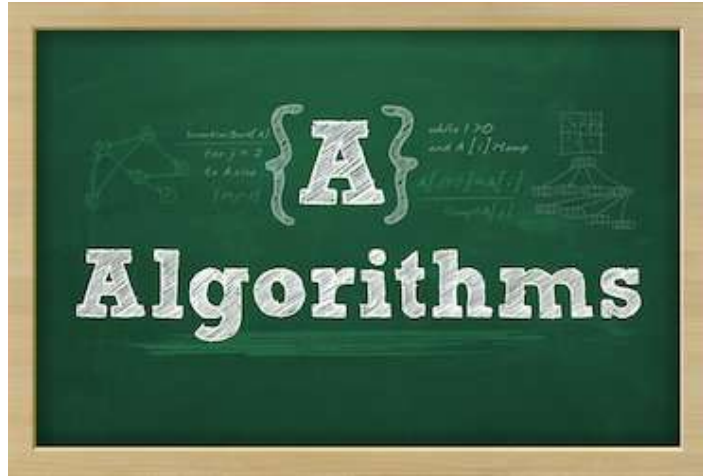
What are the Limitation?

1. **Rule Systems** are purely based on previously seen behaviour.

2. The rule systems are **deterministic**.

3. The security analyst has only **finite time**.

H₂O WORLD 2017

...therefore, what is the Problem?

1. More money, faster transactions, **lots of transactions** in a connected world.

2. **Creative ways** of committing money laundering.

3. **Too many rules.**

4. Lots of **cases to process** for analysts.

H₂O
WORLD
2 0 1 7

What is the Solution?

$$f(x)$$

What is Needed?

1. **Data** – exhaustive, quality data.

2. **Features** – quality features that **capture the nuances** in the data.

Source: Kdnuggets.com, wikimedia.org,

Features

Date	Number	Payee	Remark	Invoice	Status	Amount
01/01/2014	1001	American Insurance Group			Pending	($579.00)
01/01/2014	1003	Bob Ridden Insurance			Cleared	
01/01/2014	1004	Capital Investments			Cleared	$1,790.
01/01/2014	1005	Cedar Valley H/O Assoc.	monthly fee - Ceday Valley H/O Association		Cleared	
01/01/2014	1006	Cedar Valley H/O Assoc.	monthly dues - Ceday Valley H/O Association		Cleared	($105.00)
01/01/2014	1007	Consolidated Utility Co.	Security Lighting Fee - Account Number 300094		Cleared	($25.00)
01/01/2014	1008	Consolidated Utility Co.	Light pole photoelectric lamp - Mako Electric Company		Cleared	
01/01/2014	1009	Efficient Real Estate Company	January Service Fee for Property Management		Cleared	$2,657.
01/01/2014	1010	General Fidelity Ins.	Policy Number: 45-33445		Cleared	
01/01/2014	1011	Greater Western Agency	Policy Number: 33443-2-34444 A		Cleared	($500.00)
01/01/2014	1012	Neighborhood Monitor	monthly ad in Texas City Classified section		Cleared	($400.00)
01/01/2014	1013	Republic Mortgage	Loan Number: 660445 - A - 3304322233		Cleared	($300.
01/01/2014	1014	Resource Mortgage Co.			Cleared	
01/01/2014	1015	WestCreek Homeowner Group			Cleared	$18,450.00
01/01/2014	101041	DEPOSIT			Clear	
01/01/2014	101042	DEPOSIT			Clear	$2,550.25
01/01/2014	101043	DEPOSIT			Clear	
01/15/2014	1016	Marley Lumber Company	Materials for kitchen and bath remodeling job	IV#94323	Cleared	$19,684.25
01/20/2014	12007	DEPOSIT	CAM Charges Received for January 2007		Pending	
02/01/2014	0	DEPOSIT			Pending	($257.5
02/01/2014	1017	American Insurance Group			Cleared	($579.00)
02/01/2014	1018	Bob Ridden Insurance			Cleared	
02/01/2014	1020	Capital Investments			Cleared	$1,790.
02/01/2014	1021	Cedar Valley H/O Assoc.	monthly dues - Ceday Valley H/O Association		Cleared	
02/01/2014	1022	Cedar Valley H/O Assoc.	monthly fee - Ceday Valley H/O Association		Cleared	($542.25)
02/01/2014	1023	Consolidated Utility Co.	Security Lighting Fee - Account Number 300094		Cleared	($25.00)
02/01/2014	1024	Consolidated Utility Co.	Light pole photoelectric lamp - Mako Electric Company		Cleared	
02/01/2014	1025	Efficient Real Estate Company	February Service Fee for Property Management		Cleared	$2,657.
02/01/2014	1026	General Fidelity Ins.	Policy Number: 45-33445		Cleared	
02/01/2014	1027	Greater Western Agency	Policy Number: 33443-2-34444 A		Cleared	($500.00)

Algorithm

Algorithm

Rules + Analyst

Algorithm

Algorithm

Source: dinottelighting.com

Is this Future Proof?

Can I capture newer and creative ways of money laundering?

Source: ledvision.com.my

H₂O WORLD 2017

Anomalous Behaviour

1. Anomalies are not something that you look for outside your data.

2. They are already in your data.

3. You just need to know how to look.

A Very Simple Example

The error in the First Slide.

With Error

Corrected

1. A spelling error.
2. Due to years of reading and training our minds we identify **spelling errors** immediately. – A default context, frame of reference.

A Second Pass

Italicized

Roman

1. The letter "y" is italicized.

2. With years of training we can **almost** immediately differentiate roman and italics. Another default context, frame of reference.

A Third Pass

Font 32

Font 36

1. The letter "t" is in a smaller size font.
2. Not obvious, change of context.
3. Because we focus on the information from the text, not of the text.

Thank you.
Question?

H₂O WORLD 2017