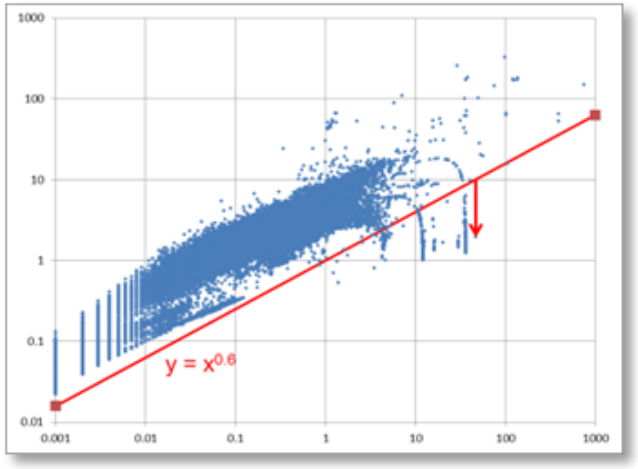
Modellen voor informatiebeveiliging en hun validatie

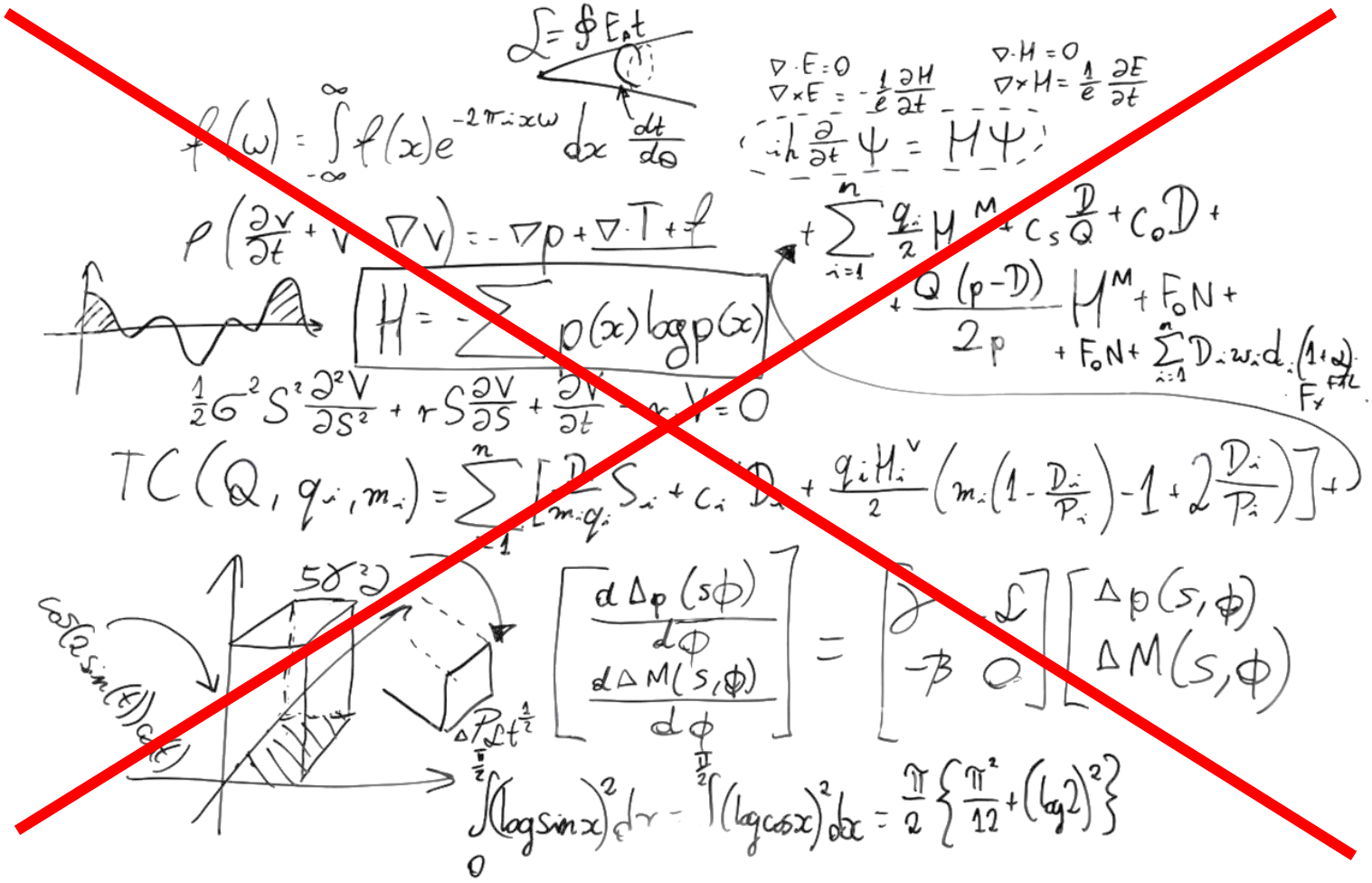
Pieter Venemans, TNO



TNO innovation for life

- TNO is een bij wet opgerichte organisatie met als doel de “BV Nederland” te ondersteunen met innovatie door middel van state-of-the art kennis.
- TNO ontwikkelt fundamentele kennis en maakt wetenschappelijke kennis toepasbaar.
- Als not-for-profit organisatie biedt TNO haar diensten kostprijs-gebaseerd aan.
- TNO ontwikkelt géén kant-en-klare producten. TNO’s rol eindigt vaak na een proof-of-concept fase

VALIDATIE VAN DATAMODELLEN...



MODELLEN

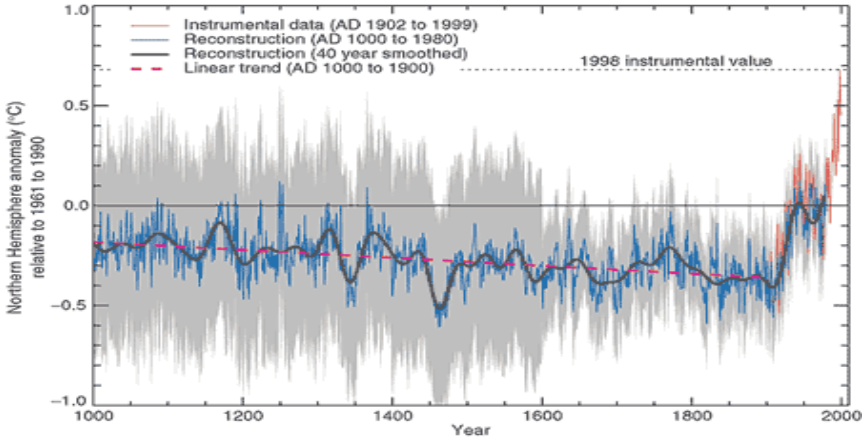
- Een model is een geabstraheerde weergave van de werkelijkheid. Een model kan formeel zijn (bijvoorbeeld een wiskundige vergelijking, een diagram of een tabel) of informeel (een beschrijving in woorden).
- Geabstraheerd = ontdaan van niet-relevante details, focus op datgene wat wij van belang achten
- Modellen kunnen gebruikt worden voor:
  - Ter vervanging van de werkelijkheid voor experimenten en voor het beantwoorden van what-if vragen
  - Het herkennen van gebeurtenissen die door een bepaald model beschreven worden
  - Het vinden van gebeurtenissen die afwijken van een bepaald model → "Anomalie-detectie"

Don't fall in love with your model

TOEPASSINGEN VAN MODELLEN

Vlucht-simulator

Klimaat-modellen

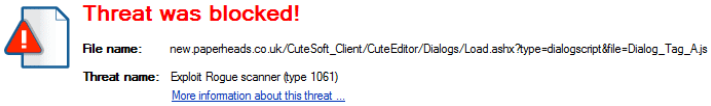


Detectie van terroristen

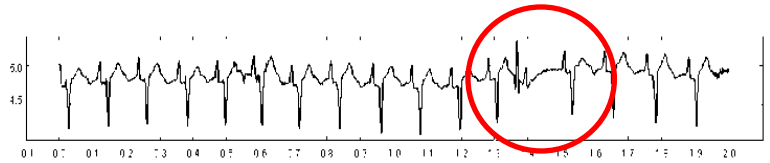
Hartbewaking

TOEPASSINGEN VAN MODELLEN VOOR INFORMATIEBEVEILIGING

- Detecteren van gebeurtenissen die matchen met een model:
  - Detectie van (bekende) virussen en andere kwaadaardige software.
  - Detecteren van (bekende) aanvalsvectoren door herkennen van bepaald gedrag (bijv port-scanning)
  - Herkennen van bepaalde (bekende) vormen van fraude

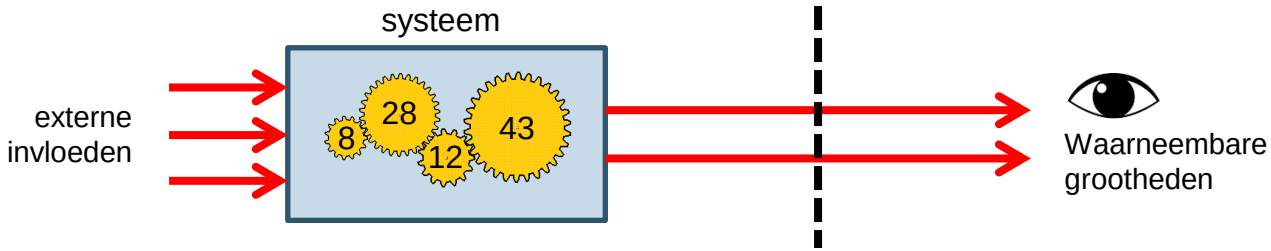


- Detecteren van gebeurtenissen die niet matchen met een model (anomalie-detectie):
  - Detecteren van onbekende aanvalsvectoren door afwijkend gedrag
  - Herkennen van onbekende vormen van fraude door gedrag dat afwijkt van wat normaal is.



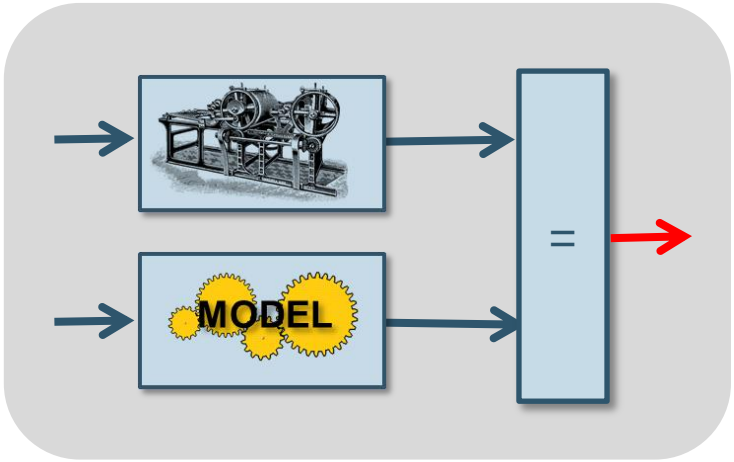
DATA- OF SYSTEEM-MODEL?

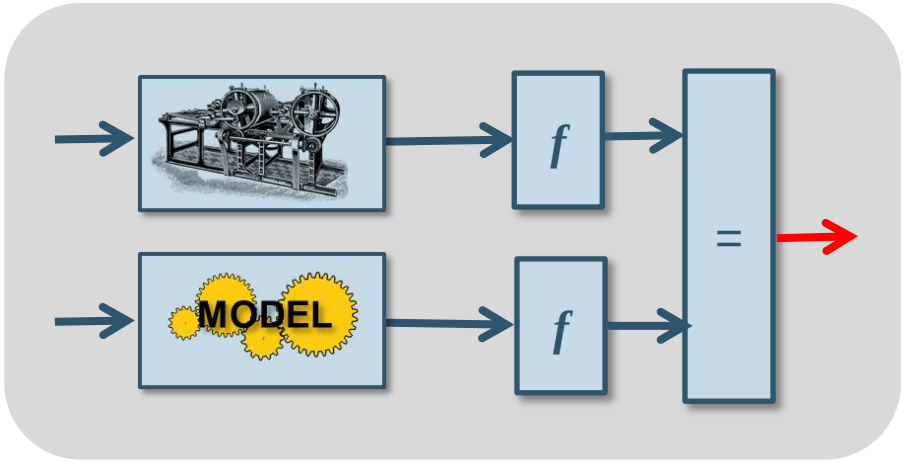
- Beschrijft een model de (waargenomen) data, of het systeem / de processen “achter de data”?
  - Vaak is het niet goed om je blind te staren op de data, zonder veel aandacht te geven aan de (onzichtbare) processen waarvan de waarnemingen de zichtbare uitingen zijn.
  - Met name een probleem als er veel stochastische processen een rol spelen, zoals bij menselijk gedrag, het klimaat enz.
  - Een goed systeem-model is vaak tijd-invariant, ondanks stochastische invloeden



VALIDATIE VAN MODELLEN

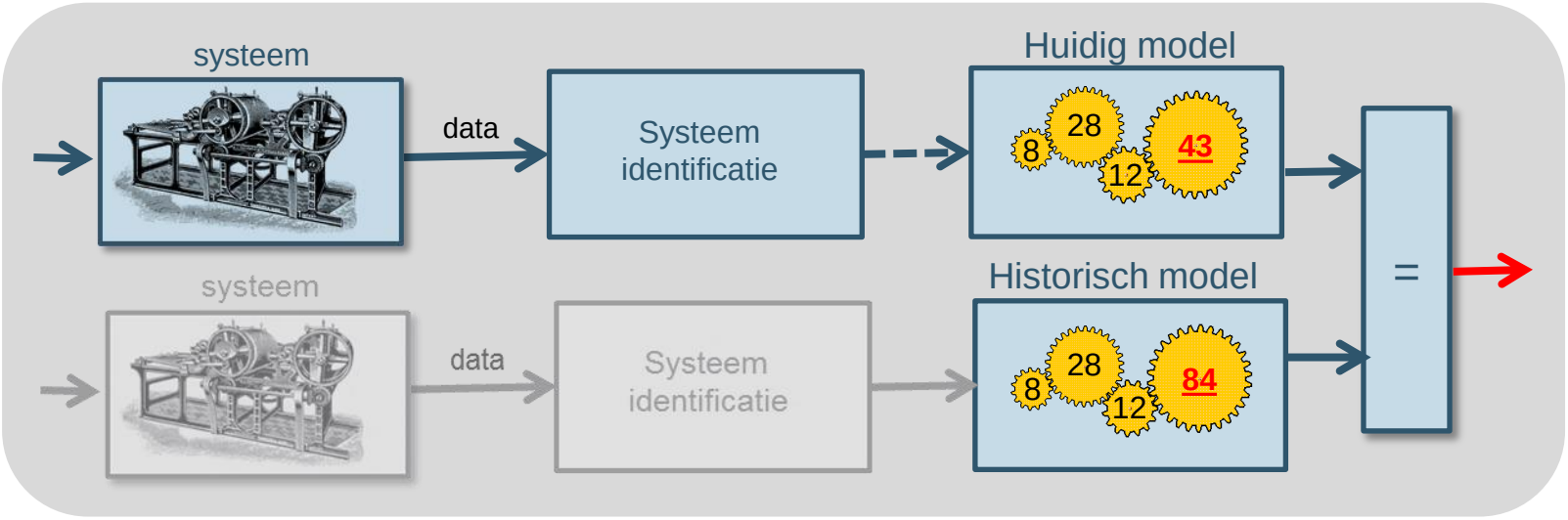
- Validatie op basis van data:
  - Produceren het systeem en het model van het systeem dezelfde data?
  - Of: dezelfde data na daar een bewerking op toegepast te hebben? (Bijv. om stochastische aspecten weg te filteren)
- Deze validatie is tegelijkertijd ook een detector!





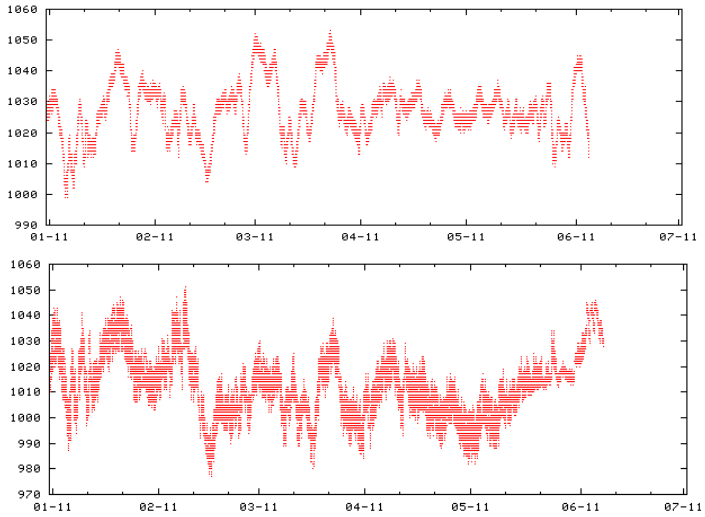
VALIDATIE VAN MODELLEN

- Validatie op basis van het model zelf:
  - Is een model van het systeem nu nog steeds gelijk aan dat van gisteren?
  - Een goed model is tijd-invariant, zolang het systeem zelf ook tijd-invariant is.
- Deze validatie is tegelijkertijd ook een (anomalie-)detector!
  - Bijvoorbeeld als de tijd-invariantie van het model plotseling doorbroken wordt



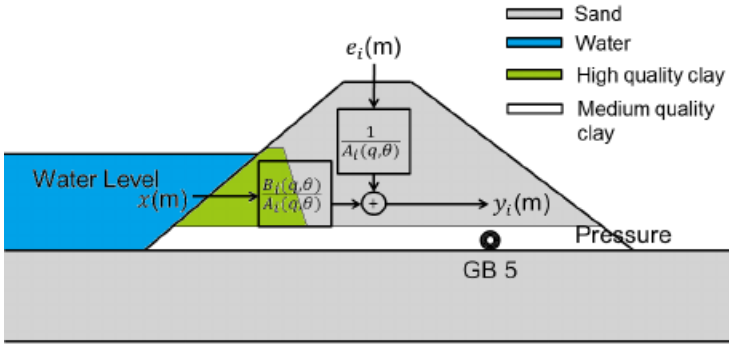
VOORBEELD 1: DIJKBEWAKING

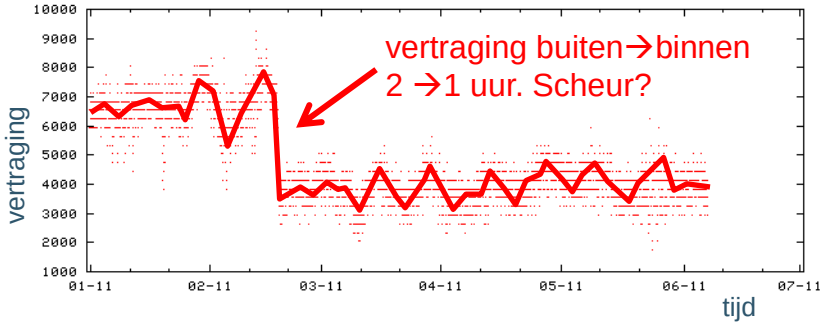
- Doel: het vroegtijdig detecteren van dijkverzwakkingen, bijv scheuren
- Dijk wordt uitgerust met een groot aantal sensoren: waterhoogte, druk, temperatuur enz.
- Voor de data (sensorwaarden) konden verschillende data scientists geen eenvoudig model afleiden: te veel invloed van getijden, temperatuur, neerslag, wind, te veel “ruis”



SYSTEEM-MODEL VOOR DIJK

- Waterdruk binnen de dijk loopt achter op de getijdebewegingen vanwege de “weerstand” van de grond en de capaciteit om water op te nemen → stelsel differentiaal-vergelijkingen
- Bepaal de parameters van het model op basis van historische data en valideer de tijd-invariantie
- Bepaal steeds opnieuw de actuele model-parameters op basis van nieuwe data
- Plotselinge veranderingen in een model parameter kunnen duiden op een scheur (of waterrat?)





VOORBEELD 2: FRAUDEDETECTIE BIJ INTERNETDIENST

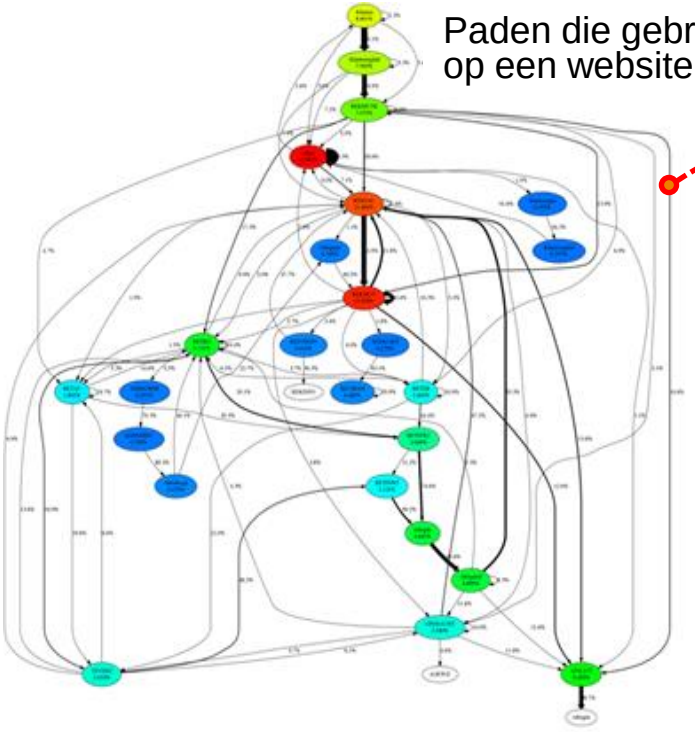
- Hypothese: fraude bij internetdienst detecteerbaar door ongebruikelijk gedrag van de klant, bijv. door ongebruikelijke navigatie op de site of door ongebruikelijke snelheid (bijv. malware die transacties tussenvoegt).

- Model: een menselijke gebruiker die een min-of-meer gebruikelijk pad doorloopt op de website, bepaalde tijd op een pagina blijft om te lezen enz.
  - Stochastisch model! Het gedrag van de gebruiker is niet te voorspellen.
  - Vormgegeven als Markov proces (Finite State machine met overgangskansen)

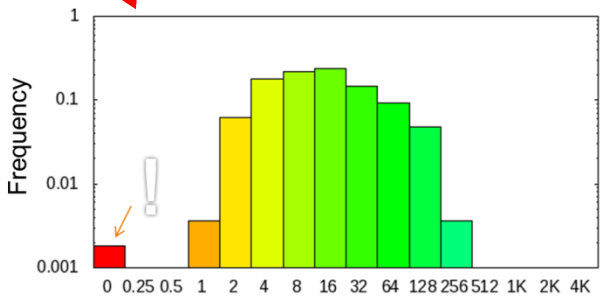
- Validatie: Tijdinvariantie van overganskansen over verschillende dagen (en daarnaast ook validatie van detector)

MODEL VOOR GEBRUIKERSGEDRAG

Markov proces (Finite State Machine + overgangskansen), aangevuld met kansverdelingen voor de “klik-snelheden” per pagina-overgang. Opgesteld op basis van historische data (kan ook “zelf-lerend)

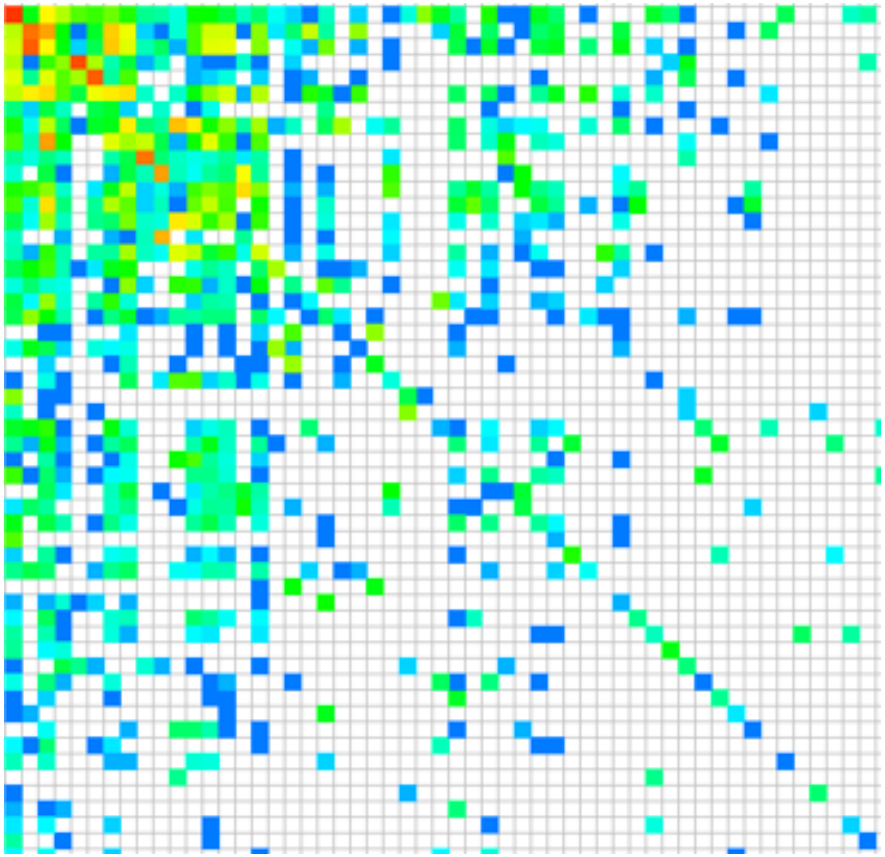


Paden die gebruikers volgen op een website.

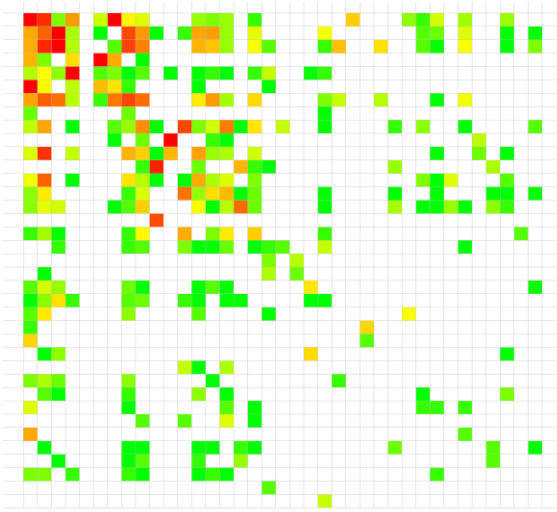


Tijd die gebruikers doorbrengen op een specifieke web-pagina voordat ze naar een andere specifieke pagina gaan

GRAFISCHE WEERGAVE VAN OVERGANGSKANSEN

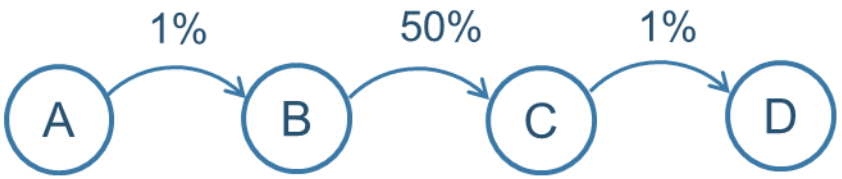


- Namen van toestanden (=pagina's) zijn hier weggelaten
- Validatie: voor verschillende dagen ziet deze figuur er min-of-meer hetzelfde uit.



DETECTOREN

- Per klantsessie: bepaal voor alle reeksen van N opeenvolgende pagina's het geometrische gemiddelde van de kans op overgangen tussen die pagina's
- Selecteer de laagste gemiddelde kans als sessie score
- Indien sessie score < drempelwaarde → anomalie

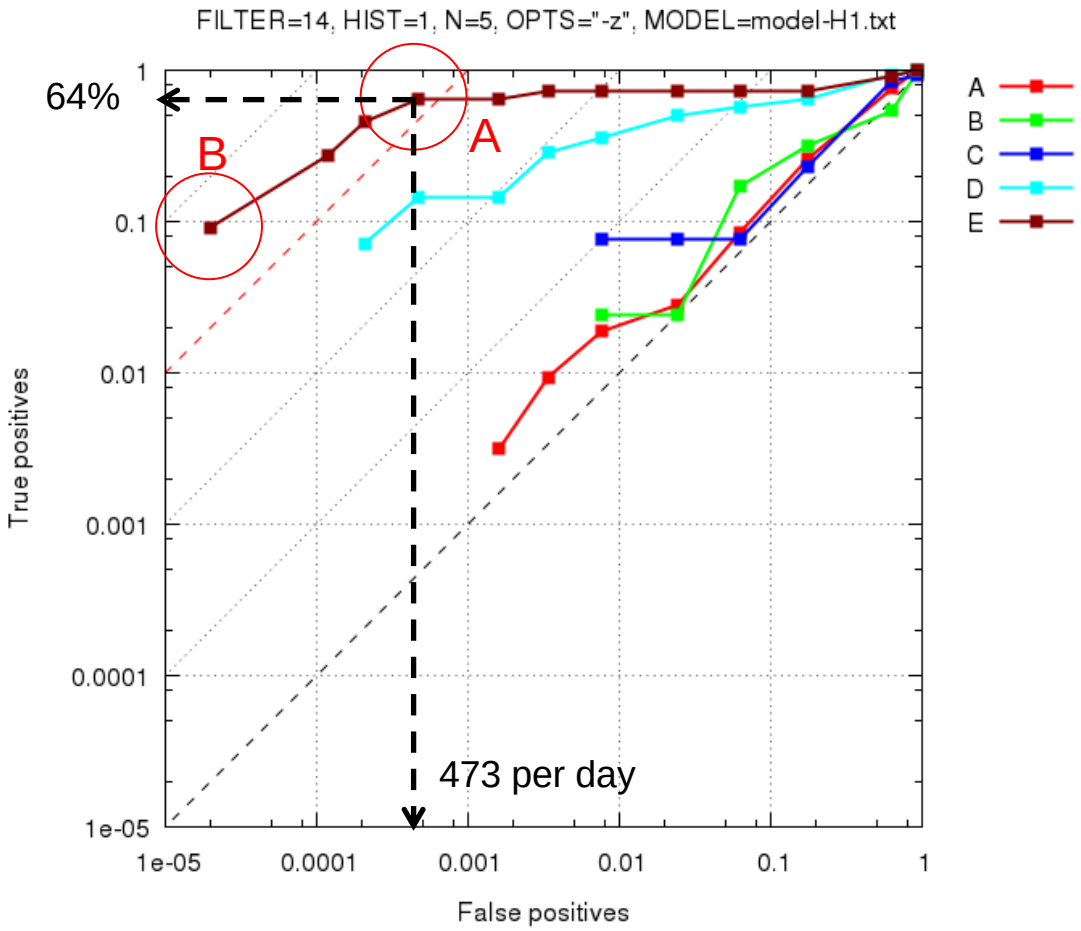


$$P = \sqrt[N]{\prod_i P_i}$$

P = 3.7%

- Validatie m.b.v. grote hoeveelheid "schone" sessies en 5 kleine sets (A, B, C, D en E) met sessies die idealiter gedetecteerd zouden moeten worden (bekende fraude-gevallen e.d.)

DETECTOR-VALIDATIE: ROC CURVES



A

	Miss	Hit
Clean	true neg 999527	false pos 473
Dirty	false neg 3.6	true pos 6.4

B

	Miss	Hit
Clean	true neg 999980	false pos 20
Dirty	false neg 9.1	true pos 0.9

Assuming 1,000,000 clean and 10 “fraud” sessions per day

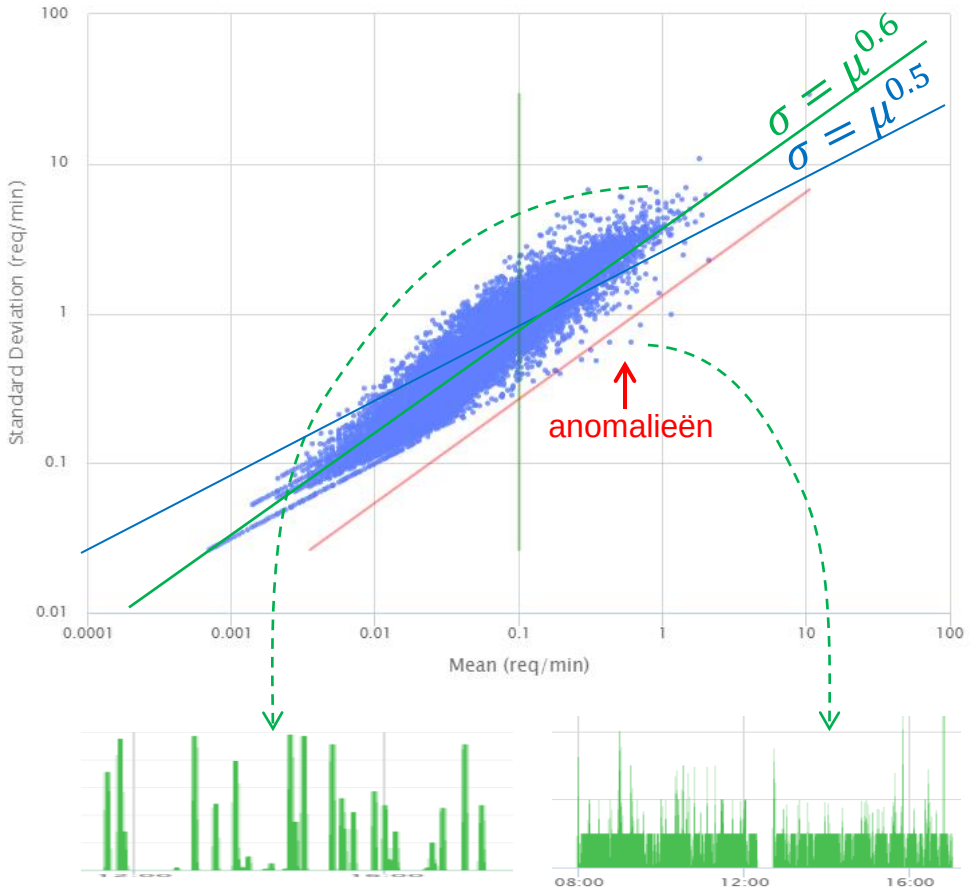
VOORBEELD 3: DNS ANOMALIE-DETECTIE

- Hypothese: diverse vormen van malware-besmettingen van werkplekken kunnen opgemerkt worden op basis van de DNS queries van die werkplekken. Hetzij door ongebruikelijke domeinnamen, of door volume, snelheid of regelmaat van de queries.

- Model: een menselijke gebruiker die met min-of-meer random tussenpozen DNS queries veroorzaakt, waarvan het merendeel “bekende” domeinen zijn (google, facebook, nu.nl)
  - Stochastisch model! Ook hier is het gedrag van de gebruiker niet te voorspellen
  - Vormgegeven als Poisson proces: geheugenloos aankomstproces met slechts één parameter, die wel voor elke werkplek anders is. Interarrivaltijd T: $P(T > t) = e^{-\lambda t}$

- Validatie: Een maat voor hoe “Poisson” het aankomstproces is.
  - Gemiddelde $\mu = \lambda$, Standaarddeviatie $\sigma = \sqrt{\lambda}$ → $\alpha = \sigma/\sqrt{\mu}$ (α=1 voor Poisson)

MODELVALIDATIE



Ieder punt representeert de DNS queries van een werkplek gedurende 24 uur.

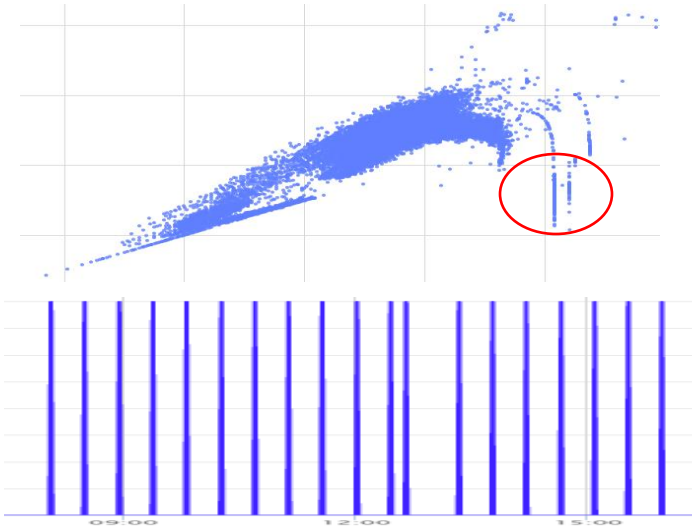
- X-as: gemiddelde
- Y-as: standaarddeviatie

Vastgesteld is dat het overgrote deel van de werkplekken binnen zekere marges voldoet aan het Poisson model (“Regression validation”)

Werkplekken met punten “buiten de wolk” bleken interessant genoeg voor het SOC (of waren servers)

DNS ANOMALIEDETECTIE

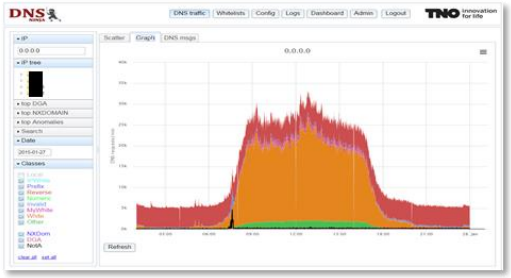
- DNS queries opgesplitst in 21 verschillende (sub)klassen: intern, whitelisted, reverse lookups, NXDomain, DGA, MX enz.
- Detector 1: werkplekken waarvan de statistieken te veel afwijken van Poisson voor één of meer van de klassen
- Detector 2: werkplekken waarvan de DNS queries een te regelmatig patroon vertonen
- Detector 3: queries naar “onwaarschijnlijke” domeinnamen (op basis van lettercombinaties & woordenboeken)
- Output: events/alerts naar SIEM voor verdere verwerking en correlatie met andere events.

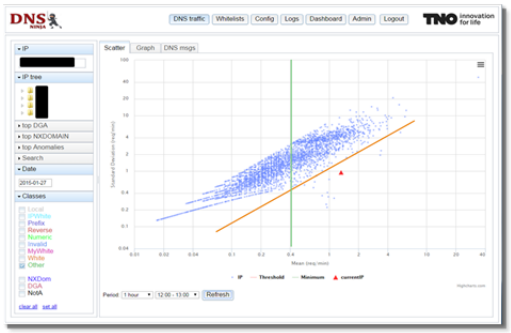


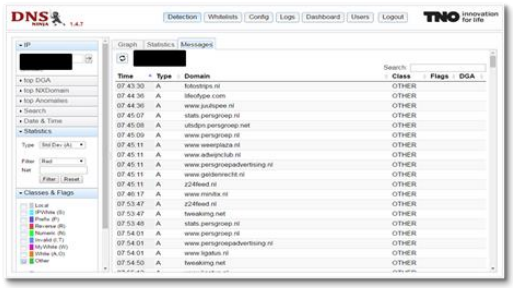
Time	Type	Domain
08:47:15	A	rgtryhbgddtyh.biz
08:49:53	A	wertdghbyrukl.ch
10:06:40	A	wertdghbyrukl.ch
11:35:19	A	wertdghbyrukl.ch

DNS ANOMALIEDETECTIE

- Het resultaat van een meerjarig innovatieproject van TNO samen met Rabobank.
- Inmiddels als 2 jaar operationeel ingezet door het SOC van Rabobank (en bij TNO)
- Bezig een volwassen product te worden. Echter: innovatie moet altijd doorgaan!







Rabobank en TNO nodigen geïnteresseerde partijen uit om deel te nemen aan het doorlopende innovatietraject.

Onder voorwaarden geen licentiekosten, slechts een (bescheiden) financiële bijdrage aan onderhoud en verdere ontwikkeling.

CONTACT

Erik Meeuwissen
Senior Consultant
Technical Sciences

T +31 88 866 77 99
M +31 6 518 955 58
E erik.meeuwissen@tno.nl

Anna van Buerenplein 1
2595 DA Den Haag
PO Box 96800
2509 JE Den Haag
The Netherlands

Pieter Venemans
Senior Research Scientist
Technical Sciences

T +31 88 866 73 07
M +31 6 519 160 63
E pieter.venemans@tno.nl

Anna van Buerenplein 1
2595 DA Den Haag
PO Box 96800
2509 JE Den Haag
The Netherlands

Kelvin Rorive
Delivery Manager
Security IT Threat Management
Rabobank - IT Infrastructure
IT Continuity & Security Services /
Cyber Defence Centre

Telefoon +31 30 21 54354
Mobiel +31 6 127 007 84
kelvin.rorive@rabobank.nl

Postbus 17100
3500 HG Utrecht
Croeselaan 18
3521 CB Utrecht


BEDANKT VOOR UW AANDACHT
Voor meer inspiratie:
TIME.TNO.NL
TNO
innovation
for life