RegCheck: risicobeoordeling van nieuwe .nl-registraties

Thymen Wabeke | Security Academy Unlocked

31 mei 2023

Aanleiding RegCheck

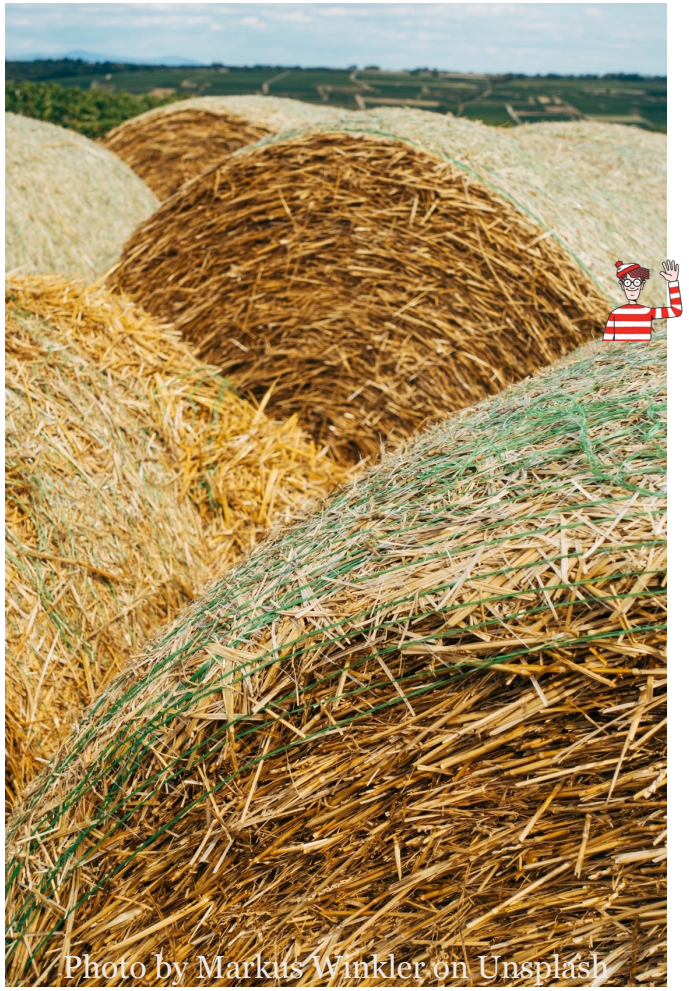
- SIDN staat voor een veilig .nl-domein

- Malafide intenties soms vrij duidelijk
  - Risicovolle domeinnaam
  - Ongeldige houdergegevens

Dus… Waarom wachten tot de abusemelding?

- Proactief valideren van domeinnaam registraties maakt .nl veiliger

- Handmatige alles controleren is geen optie:
  - Ruim 2.000 registraties per dag
  - Slechts 3 registraties hiervan binnen 30 dagen op Netcraft (0,15%)



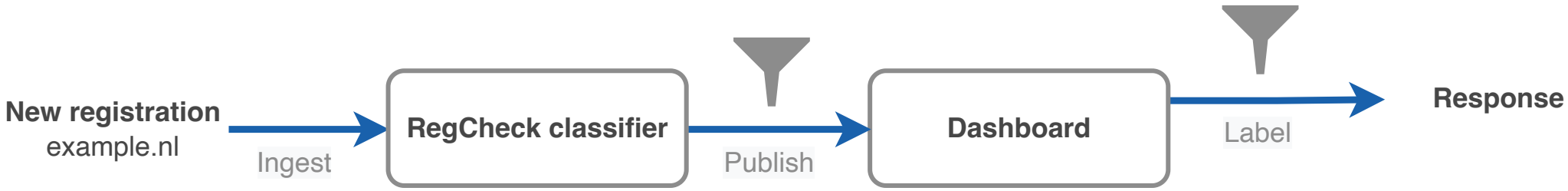
Op het menu…

Methode en resultaten

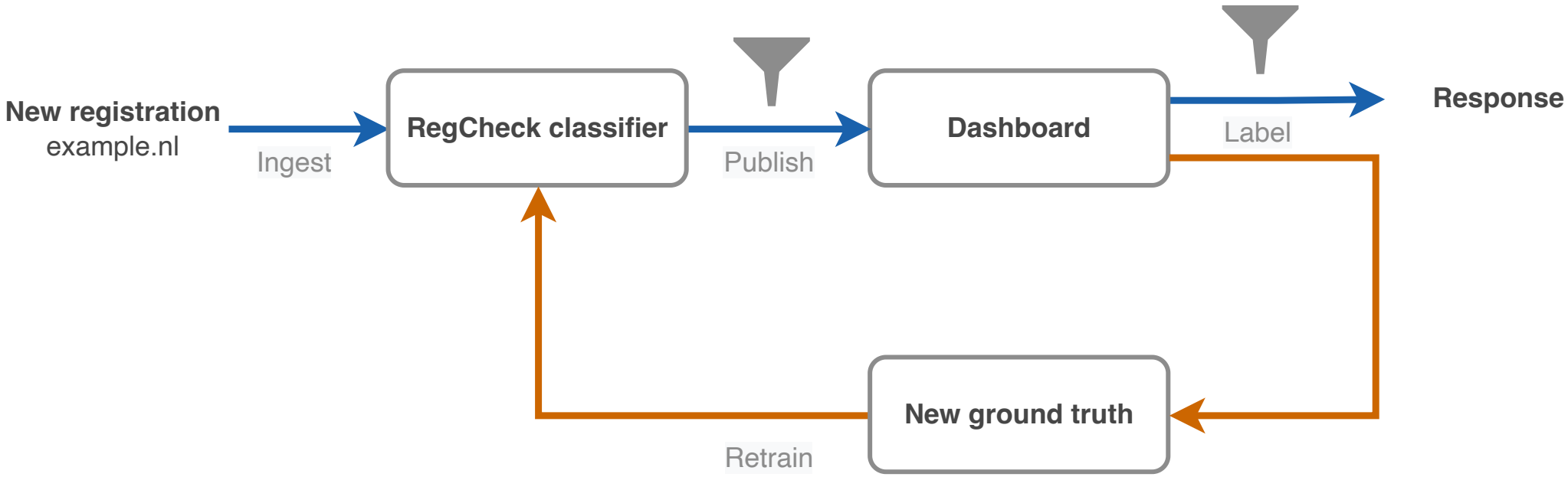
Vier lessen

Photos by Amélie Mourichon and Brett Jordanon on Unsplash

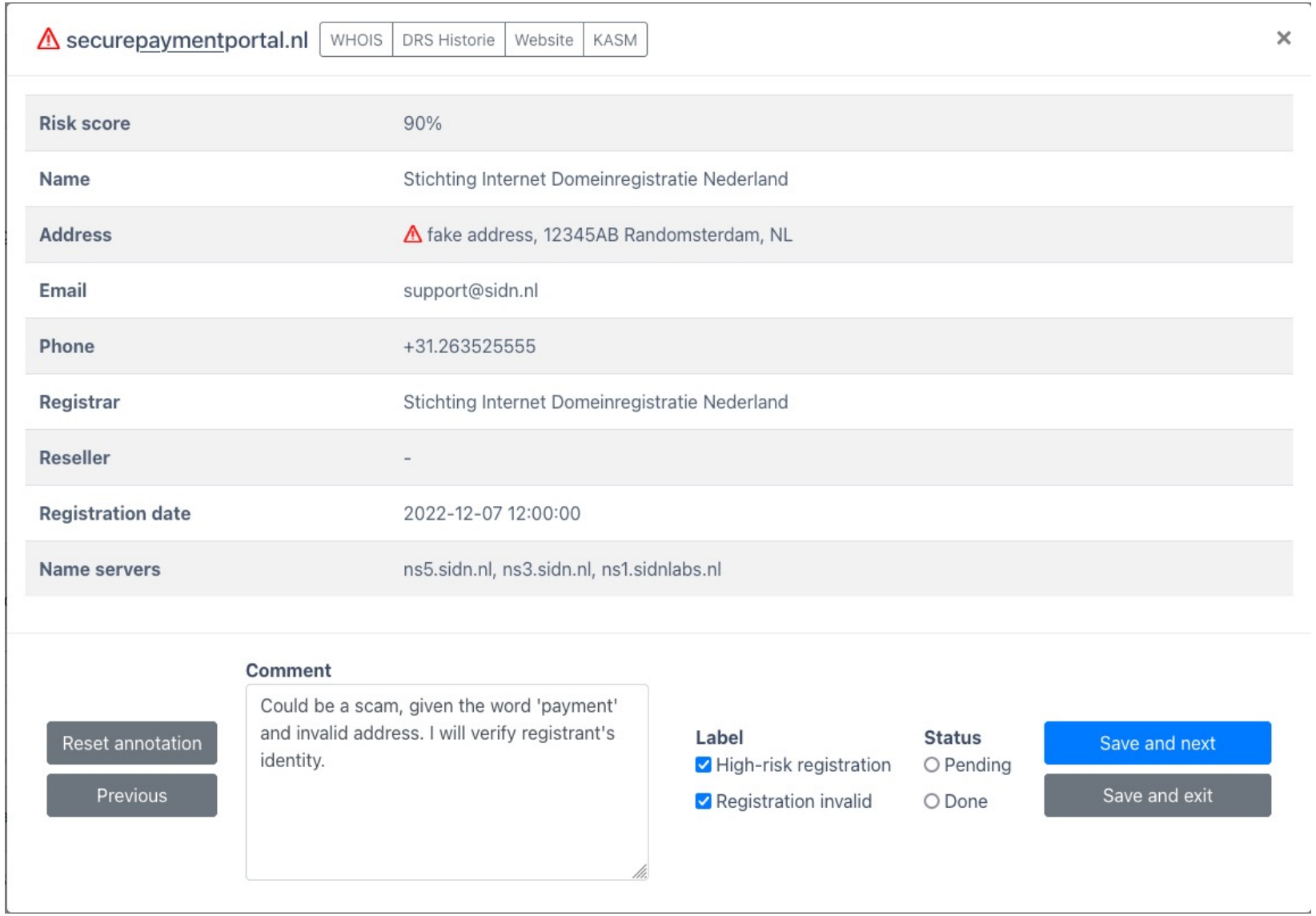
RegCheck: potentieel malafide registraties filteren



RegCheck: potentieel malafide registraties filteren



Dashboard


securepaymentportal.nl
WHOIS
DRS Historie
Website
KASM
Risk score
90%
Name
Stichting Internet Domeinregistratie Nederland
Address
fake address, 12345AB Randomsterdam, NL
Email
support@sidn.nl
Phone
+31.263525555
Registrar
Stichting Internet Domeinregistratie Nederland
Reseller
-
Registration date
2022-12-07 12:00:00
Name servers
ns5.sidn.nl, ns3.sidn.nl, ns1.sidnlabs.nl
Comment
Could be a scam, given the word 'payment' and invalid address. I will verify registrant's identity.
Reset annotation
Previous
Label
High-risk registration
Registration invalid
Status
Pending
Done
Save and next
Save and exit

Berekening risico

- Risicofactor: kenmerk dat risico verhoogt (21 momenteel)
- Verschillende regel-gebaseerde en machine learning classifiers verkend
- Sinds augustus ’22 een logistische regressiemodel in gebruik
- Registry onafhankelijke code

Offline en online resultaten

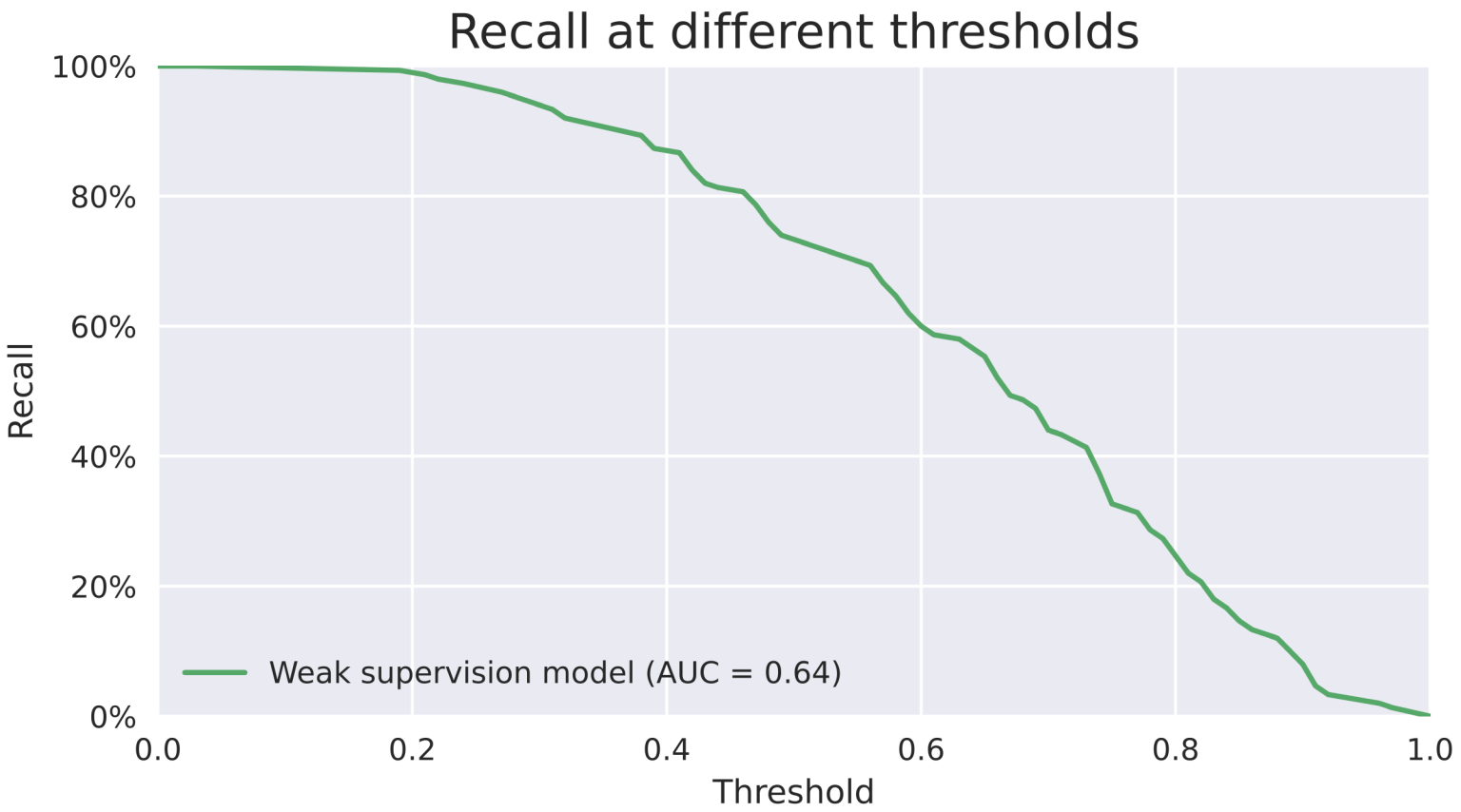
	Machine learning	Rule based
Recall	48%	9%
PPV (precision)	22%	0.55%

Table 1: RegCheck's results on historical data (August to November 2022).

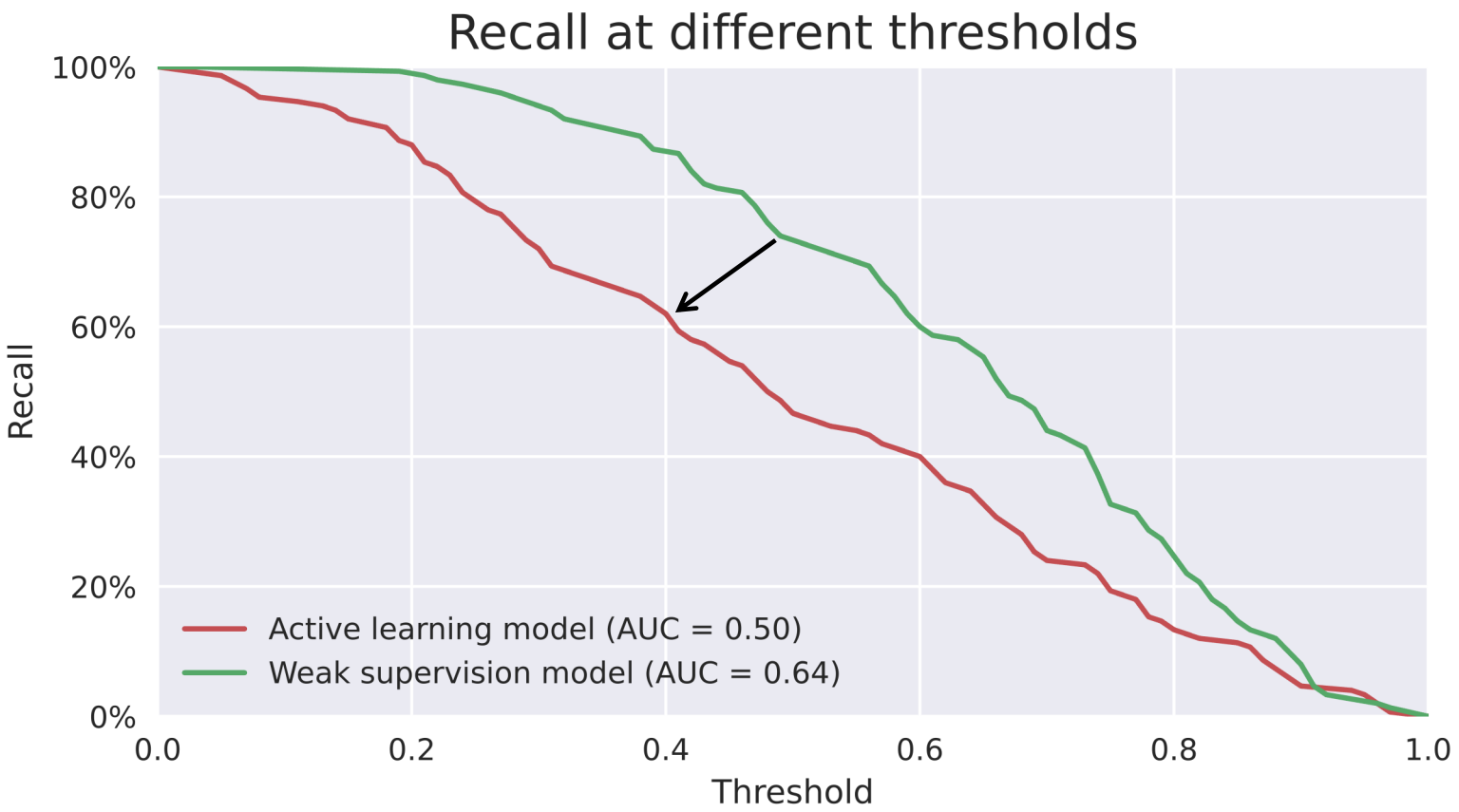
	Machine learning
Registrations	43k
High-risk classifications	181 (0.4%)
True positives	38 (21%)

Table 2: RegCheck's results on new registrations (17 November to 8 December 2022).

Effect van feedback loop (1/2)



Effect van feedback loop (2/2)



Les 1: Spreek dezelfde taal

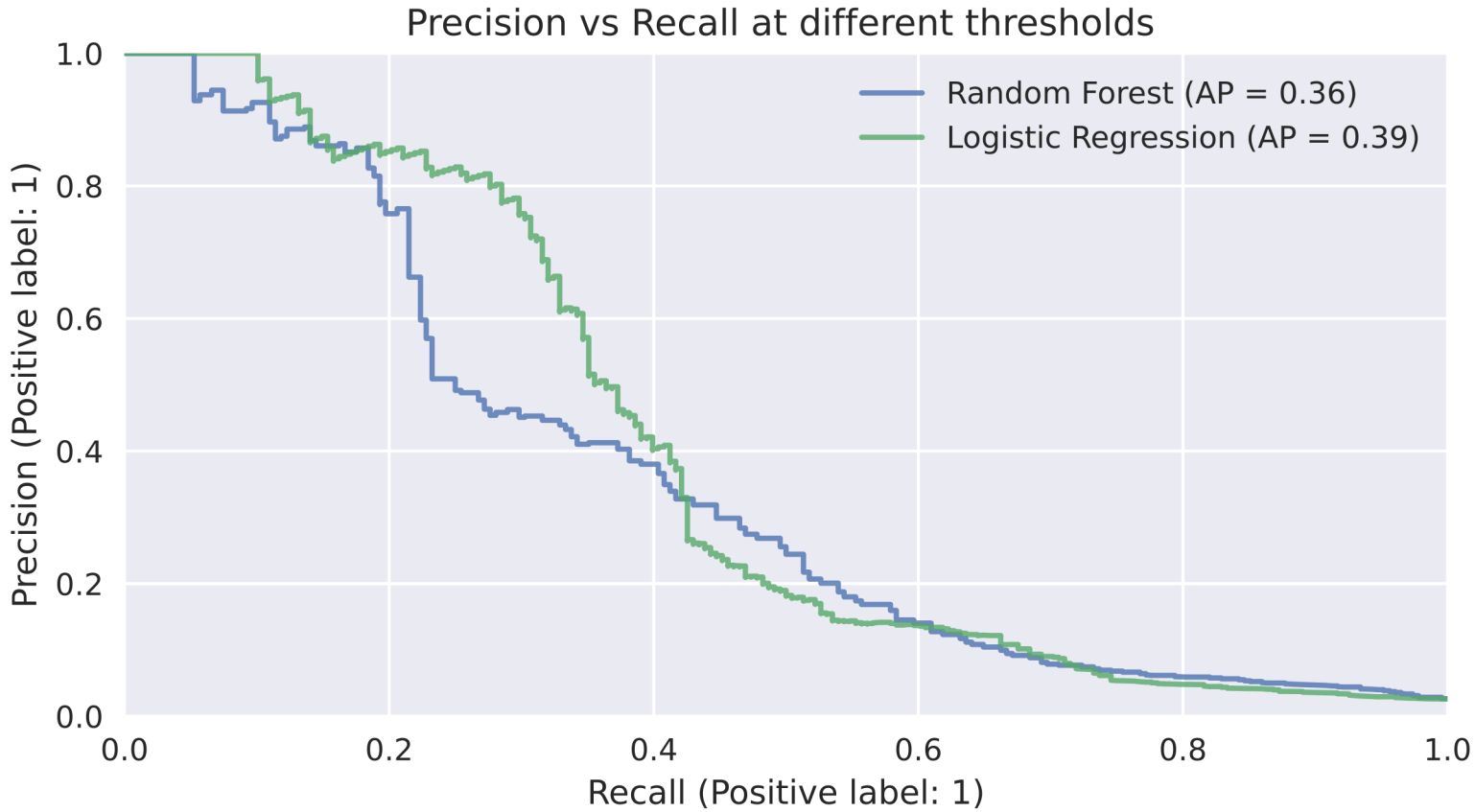
Photo by Tim Schmidbauer on Unsplash

- Probleemdefinitie [1]
  - Domeinnamen verdacht van abuse detecteren?
  - Domeinnamen met ongeldige houdergegevens detecteren?

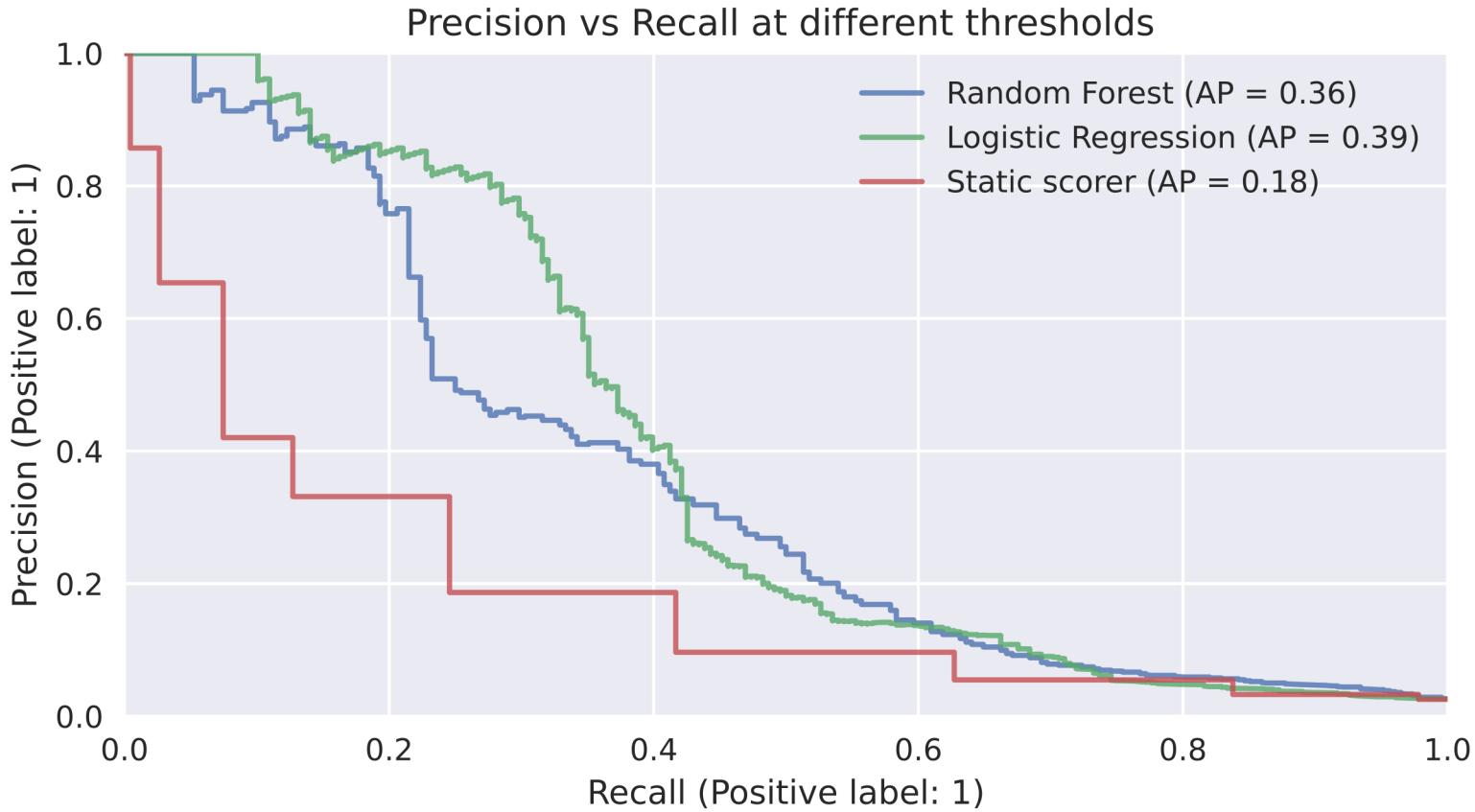
- Goed gedefinieerde uitkomsten
  - Wat betekent “verdacht”?
  - Maakt iedereen dezelfde beslissingen?

[1] Problem Formulation and Fairness - https://arxiv.org/abs/1901.02547

Bepalen van performance (1/2)



Bepalen van performance (2/2)



Les 2: Benchmark ML tegen niet-ML baseline


Photo by Hasan Almasi on Unsplash

- Complexe ML algoritmes zijn niet altijd beter dan eenvoudige alternatieven (bijv. uitlegbaarheid, hogere kosten) [2]

- Een niet-ML baseline brengen voor- en nadelen van ML beter in kaart

[2] Measuring the predictability of life outcomes with a scientific mass collaboration - https://www.pnas.org/doi/10.1073/pnas.1915006117

Les 3: Interpreteren van interpretaties niet triviaal

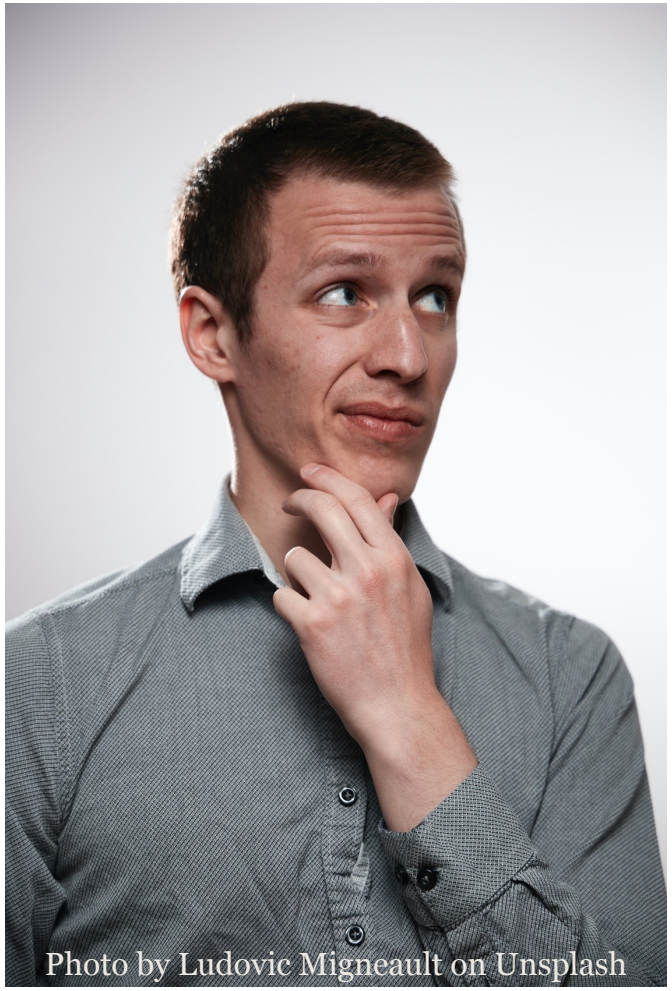


Photo by Ludovic Migneault on Unsplash

- Uitlegbare risicoscores ingewikkeld, zelfs als het ML algoritme intrinsiek te interpreteren is
- Hoe voorkom je dat de uitleg misleidend is (bijv. suggestie van causaliteit, interactie tussen risicofactoren)?
- Helpen interpretaties daadwerkelijk om fouten te detecteren? [1, 2]

[1] Manipulating and Measuring Model Interpretability - https://arxiv.org/abs/1802.07810
[2] Interpreting Interpretability - https://dl.acm.org/doi/abs/10.1145/3313831.3376219

Les 4: Discussieer technische keuzes en hun impact

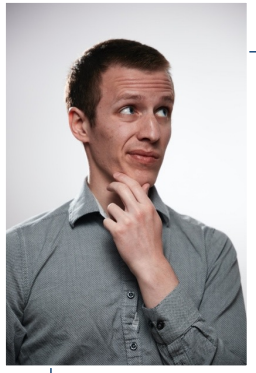

Photo by Clay Banks on Unsplash

- Technische keuzes hebben invloed op processen en beleid (bijv. drempelwaardes, features)
- Verantwoord gebruik van machine learning alleen mogelijk als beslissingen expliciet worden gediscussieerd en bekeken van meerdere kanten

Vier lessen

Spreek dezelfde taal

Benchmark met niet-ML baseline



Interpreteren van interpretaties niet triviaal

Discussieer technische keuzes & impact

Plannen voor 2023+

- Prototype blijven gebruiken en verbeteren
- Mogelijk automatisch houderonderzoek starten
- Gezamenlijke ontwikkeling en evaluatie met DNS Belgium (.be)
- Andere registries helpen door code te delen

Photo by Jess Bailey on Unsplash

Q&A

https://www.sidnlabs.nl/nieuws-en-blogs/risicobeoordeling-van-nieuwe-nl-registraties-met-behulp-van-regcheck

thijs.vandenhout@sidn.nl
thymen.wabeke@sidn.nl