



existentia

propositum

operatio



Brenno de Winter

- Schreef eerste code toen ik 5 jaar oud was
- Hacker
- 15 jaar onderzoeksjournalistiek, Journalist van het Jaar 2011
- Chief Security and Privacy Operations at Ministerie van VWS
- Werk als zelfstandige
- Veel security onderzoek



VOLG ONS:



Volgend bericht Gebruik sterke wachtwoorden en houd ze veilig >

< **Vorig bericht** Het sprookjesdier

UITGELICHT

Neus voor slechte zaken

DOOR KEIKO · 24/10/2022

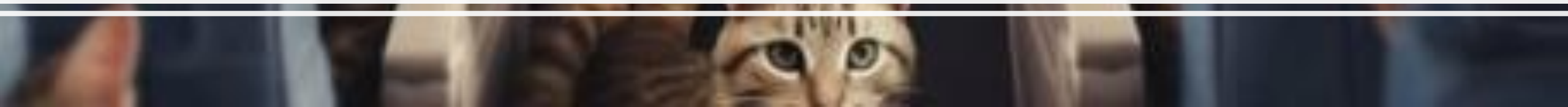








Hoe het ooit begon





Stop met janken



Coronamelder: privacy first, security first

Design

- Decentraal systeem
- Geen informatie vragen aan gebruikers
- Strakke retentie
- Zo moeilijk mogelijk te linken aan persoon
- Geen identifiers op op apparaat
- Alleen noodzakelijke data
- Alleen data doorgeven na verificaties
- App ziet geen codes

Gevalideerd

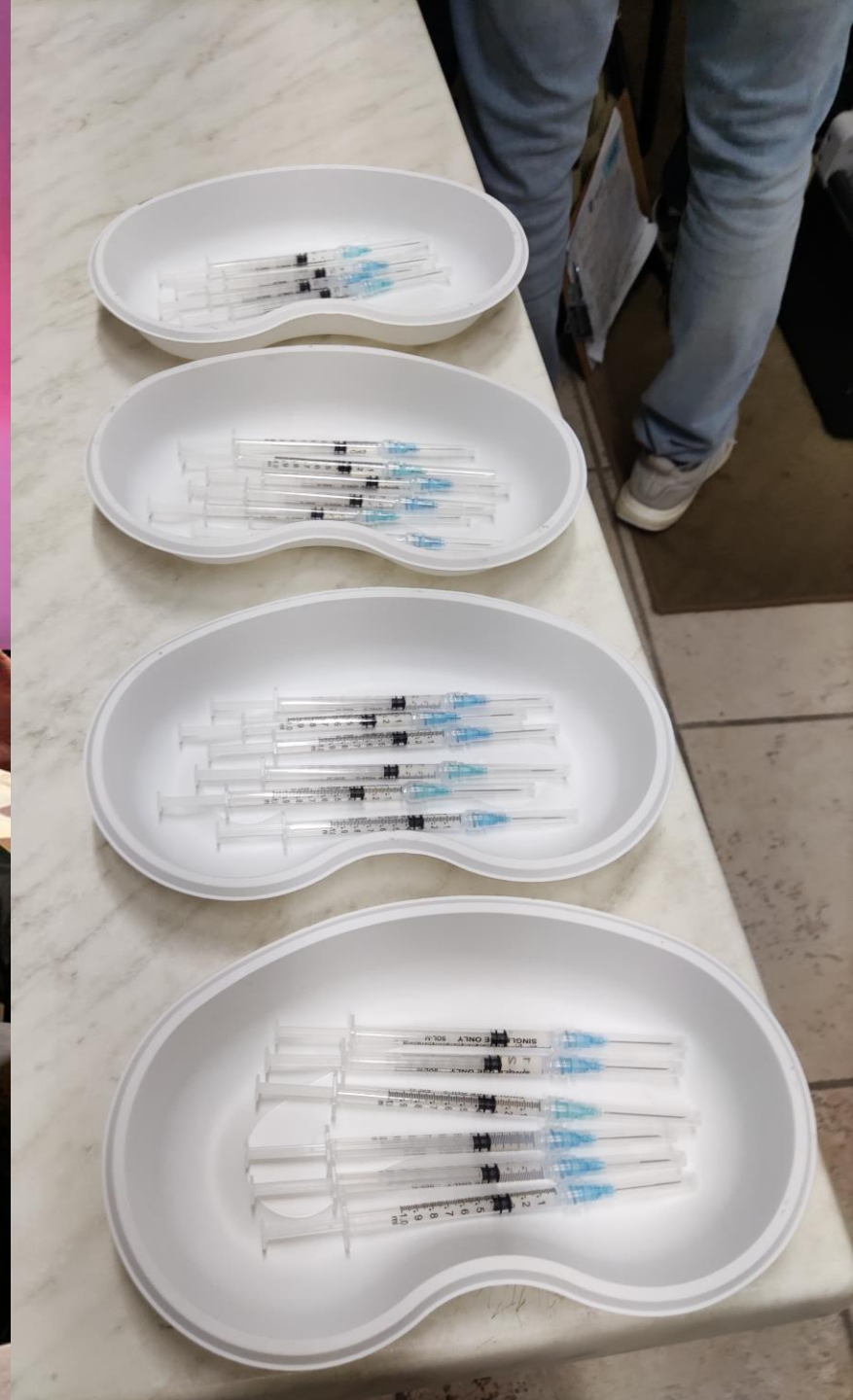
- Doelbinding in de wet
- Strafbepaling
- Geen statistieken feest
- Cryptografisch correct (alles signen)
- Geen backups maken
- Detecteren op misbruik

Word gewaarschuwd

Weet wanneer je extra kans op besmetting hebt gelopen



Bewijzen dat je
gevaccineerd
bent

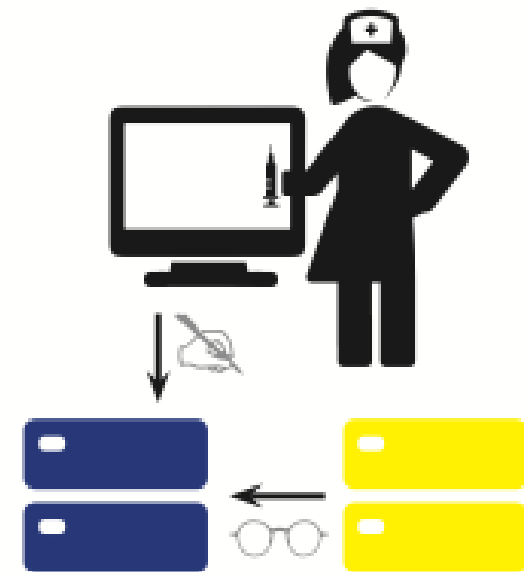


Registratie van vaccinaties met *state-of-the-art security*



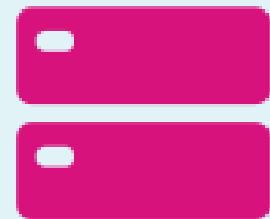
Rijksoverheid

Invoer vaccinatie via webbrowser



Branie
zet versleutelde
data klaar voor
validatie in Database.

Bananie
haalt data op
voor validatie in
opdracht van Zeiko.



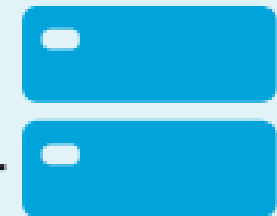
Zeiko

- valideert data
- notificatie aan medewerker via Bananie aan Branie
- plaatst gevalideerde data in Database



**Versleutelde
database met
vaccinregistraties**

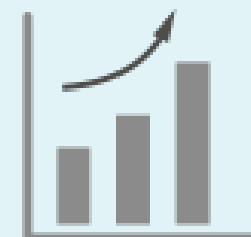
Opvragen data via webbrowser of veilige verbinding



Keiko

leest de database
voor automatische
of handmatige
dataverzoeken.

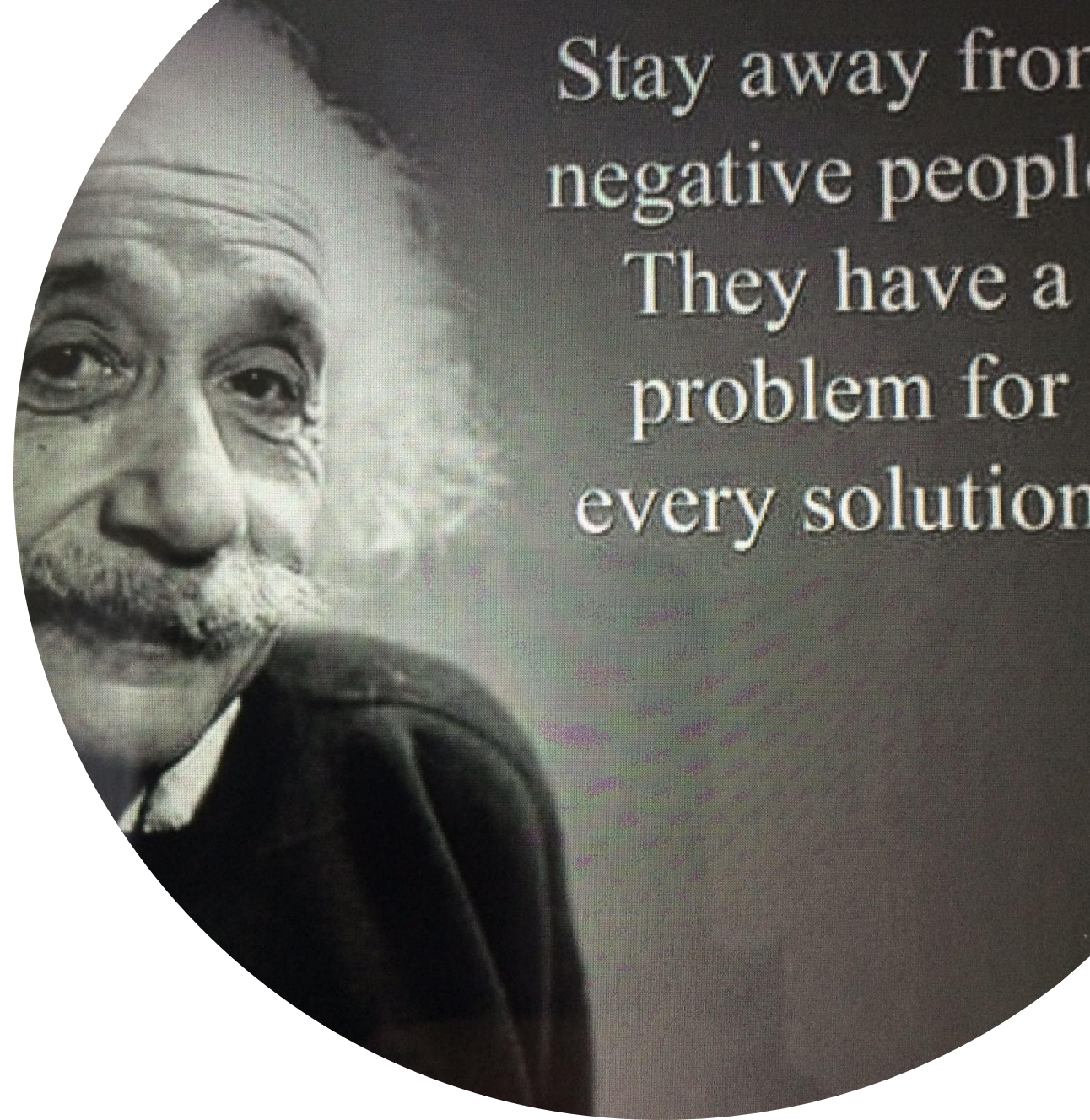
```
10101100011001101
10101101010001101
10101111011001101
101011010001101
101110000001101
```



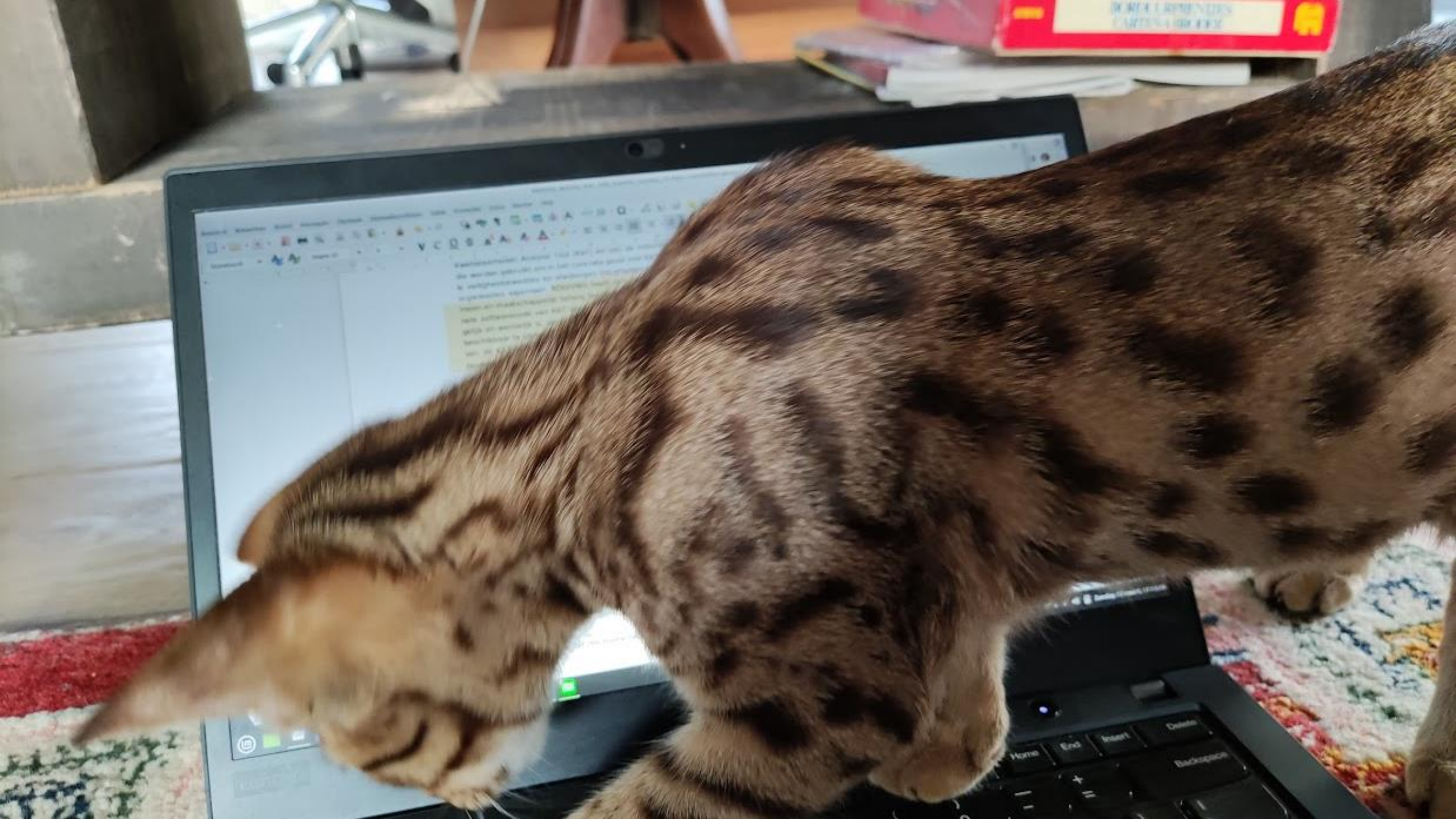
Falen centraal stellen

Failure Mode Effect Analysis

- Ernst 1-5 – Hoe hoger hoe ernstiger
- Voorkomen 1-5 – Hoger betekent meer voorkomend
- Detecteerbaarheid 1-5 – Hoe hoger hoe moeilijker te detecteren









Just the facts!

Uniform pentesten


- Uniforme eisen voor inkoop van pentesten
- Alle bevindingen langs dezelfde meetlat (CVSS)
- Een minimale set aan eisen:
 - OWASP TOP-10
 - MSTG/WSTG
- Uniforme manier van presenteren van bevindingen: PTES
- Reproduceerbaarheid van het onderzoek
- Het rapport wordt openbaar



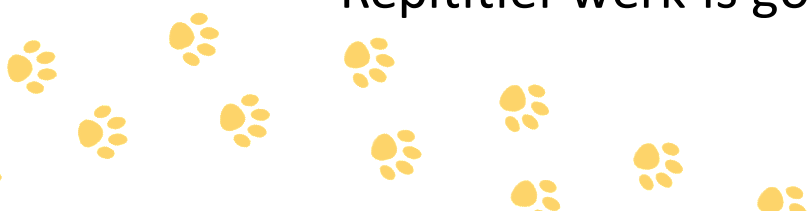


Oude neigingen doorbreken

- Informatiebeveiliging is een vak
 - Dezelfde vraagstukken telkens weer blijven beantwoorden
 - Iedere keer rapporten kloppen in word met vergelijkbare inhoud
 - Rapportages met hard bewijs zijn lastig te vinden
 - Vaak zijn het antwoorden op vragen, niet feiten
 - Veel tools kiezen kortste route naar antwoord
 - Technische feiten hebben weinig relatie met normatieve controls
- Positief
 - Er zijn veel tools beschikbaar die feiten kunnen verzamelen
 - Veel tools zijn open source
 - Data is goed te modeleren
 - Repititief werk is goed te automatiseren



Ambachtelijk
automatisering
is niet vol te
houden.





Prima





Compliance is



Just
the
facts!

Wie heeft een up-to-date CMDB?

En wie loopt hier onjuistheden te verkondigen?





Zoek een speld in de hooiberg

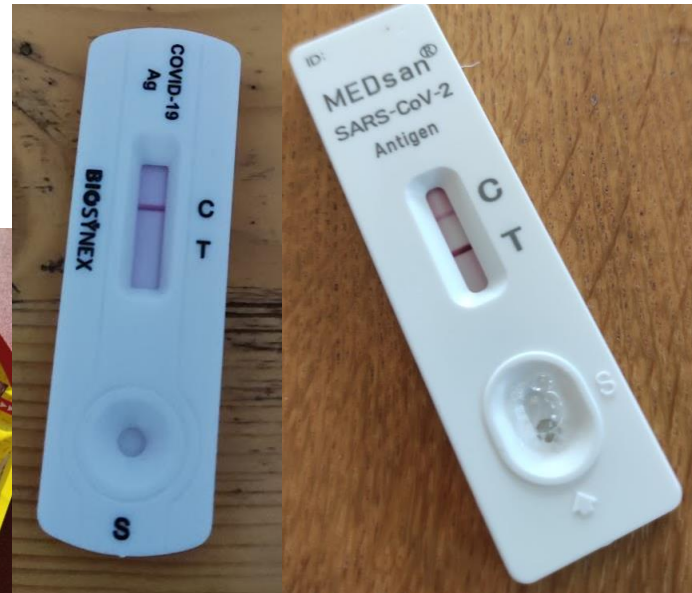


Zoek Franse worstjes in een
hooiberg



Zoek een sok in de hooiberg

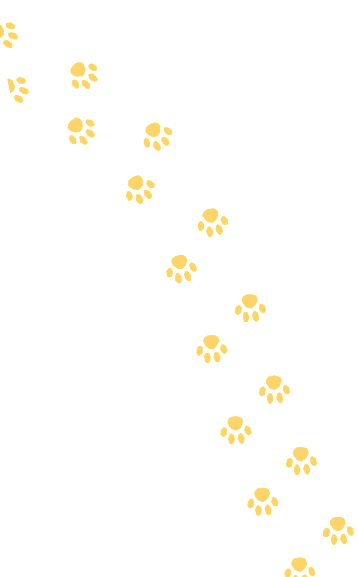
Feiten in Octopoes



Sorteer objecten en plaats ze waar ze horen

- Bi-Temporal graph database
 - Objecten zijn feiten
 - Met timestamps wanneer iets voor het eerst is gezien en wanneer het werd verwerkt (gerealiseerd)

Just the facts!

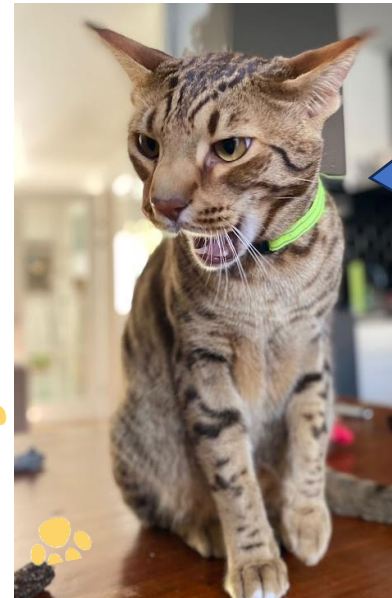
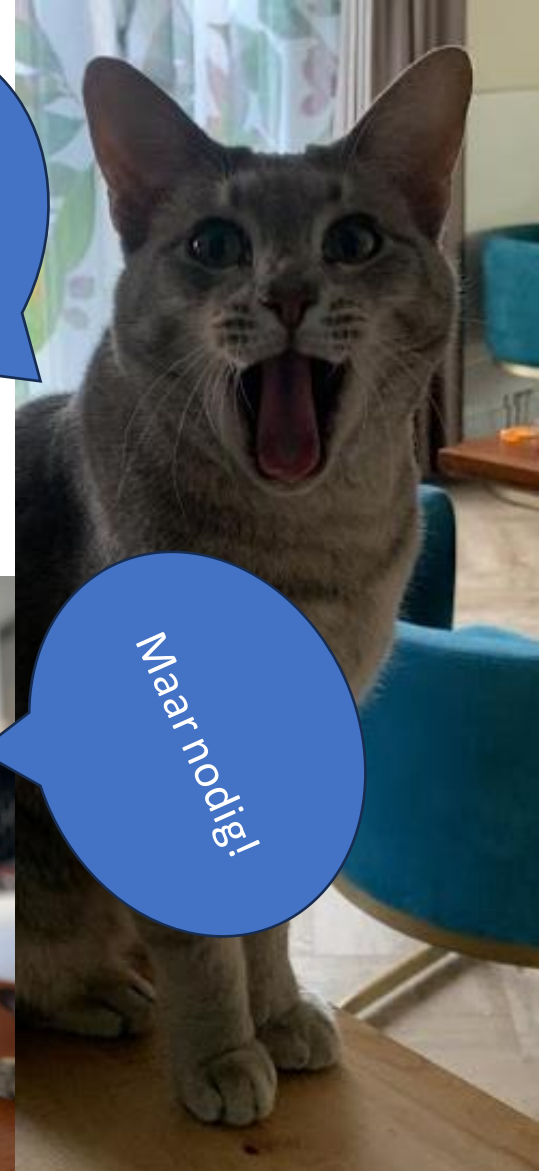
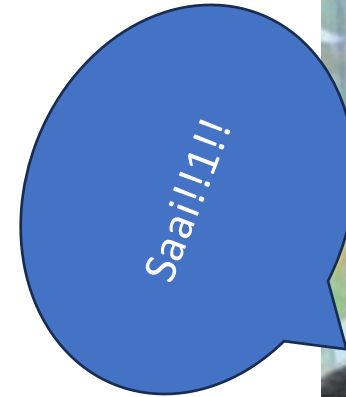


Hoe bewijs je de feiten die je claimt?

Bij iedere stap:

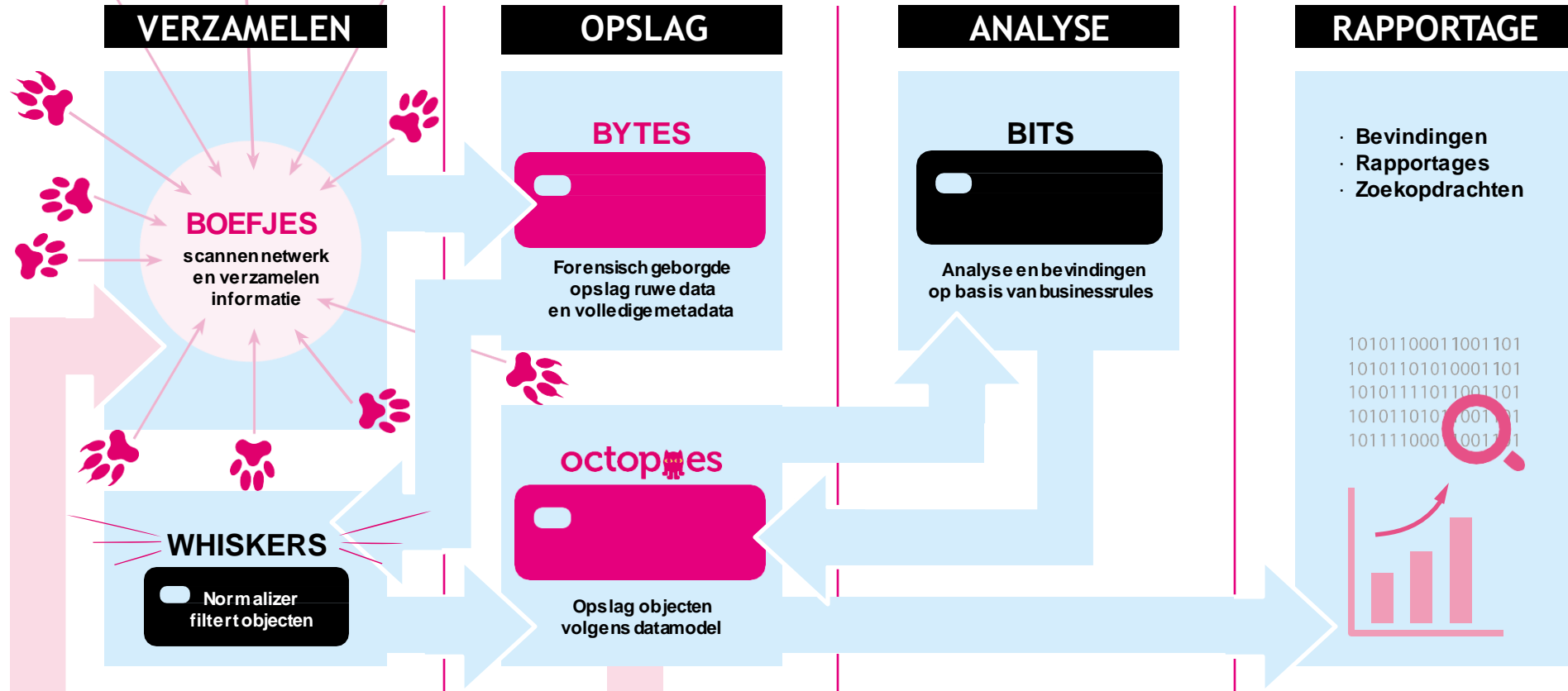
- Maak je onweerlegbaar bewijs
- Hashen waar het kan
- Hashes worden extern gesigned

Jezelf hoef je niet te overtuigen,
Overtuigen doe je bij iemand anders





Modules OpenKAT Kwetsbaarheden Analyse Tool



Per gevonden object worden op basis van het datamodel nieuwe boefjes uitgestuurd.



Een overzicht van alle beschikbare boefjes. Boefjes kunnen worden gebruikt om te scannen op kwetsbaarheden en beveiligingsproblemen binnen gespecificeerde objecten. Elk boefje heeft zijn eigen toepassing.

39 Beschikbare plug-ins

Filteropties tonen 



Vrijwaringsniveau: 

ADR Finding Types

Hydrate information of ADR finding types

Uitgever: OpenKAT

[Zie details](#)

Uitschakelen



Vrijwaringsniveau: 

API Design Rules validator

Validate if an API conforms to the API Design Rules

Uitgever: OpenKAT

[Zie details](#)

Inschakelen



Vrijwaringsniveau: 

BinaryEdge

Use BinaryEdge to find open ports with vulnerabilities that are found on that port

Uitgever: OpenKAT

[Zie details](#)

Inschakelen



Vrijwaringsniveau: 

Censys


Use Censys to discover open ports, services and certificates

Uitgever: OpenKAT

[Zie details](#)

Inschakelen



Vrijwaringsniveau: 

CRT

Certificate search

Uitgever: OpenKAT

[Zie details](#)

Uitschakelen



Vrijwaringsniveau: 

CVE_2023_35078

Use NFIR script to find CVE-2023-35078

Uitgever: OpenKAT

[Zie details](#)

Inschakelen



Vrijwaringsniveau: 

CVE Finding Types

Hydrate information of CVE finding types from the CVE API

Uitgever: OpenKAT

[Zie details](#)

Uitschakelen



Vrijwaringsniveau: 

CWE Finding Types

Hydrate information of CWE finding types

Uitgever: OpenKAT

[Zie details](#)

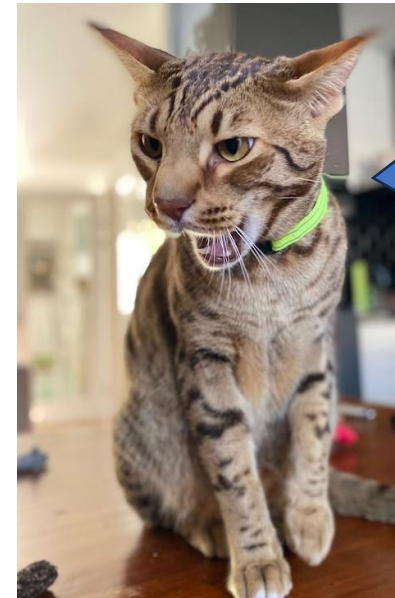
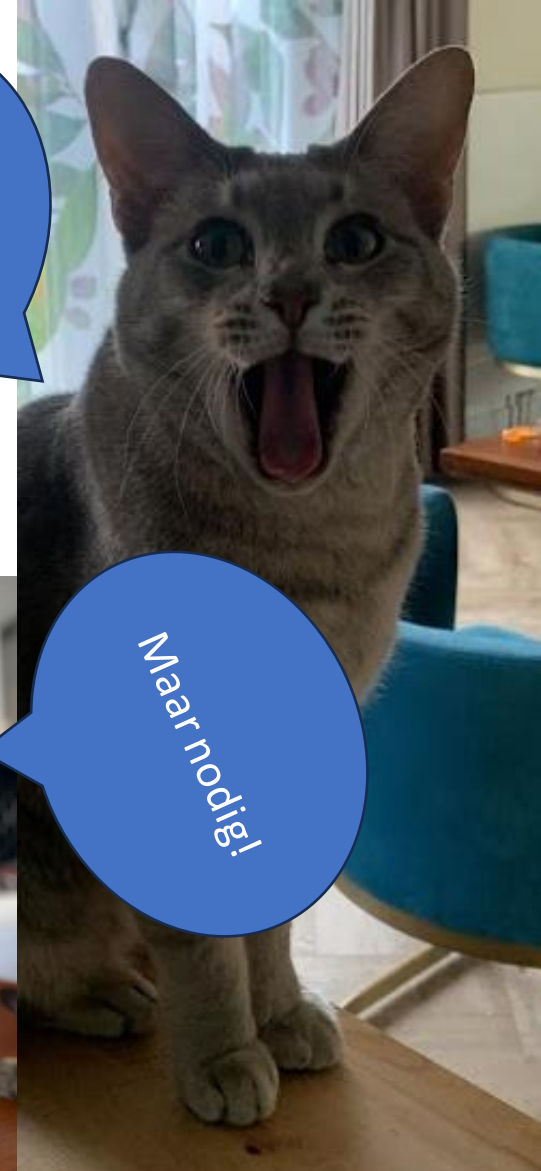
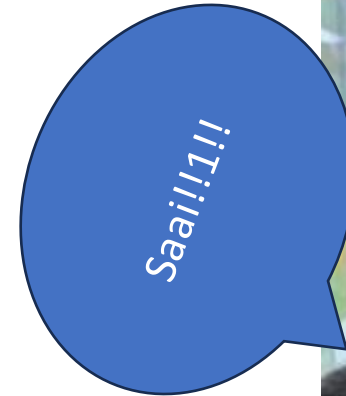
Uitschakelen

Hoe bewijs je de feiten die je claimt?

Bij iedere stap:

- Maak je onweerlegbaar bewijs
- Hashen waar het kan
- Hashes worden extern gesigned

Jezelf hoef je niet te overtuigen,
Overtuigen doe je bij iemand anders

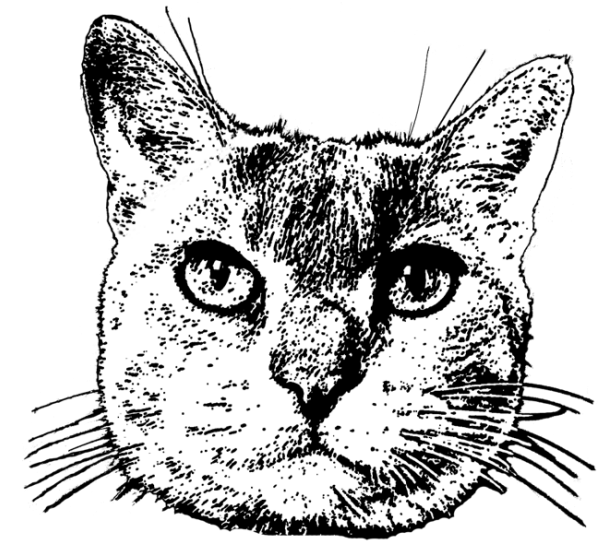




Just the facts!

OpenKAT is een reeks projecten

- Momenteel in OpenKAT
 - Bits – Business rule engine
 - Boefjes – API-infrastructuur
 - Bytes – Forensische documenten opslag
 - Maya – Documentatie
 - Mula - Scheduler
 - Octopoes – Temporal graph database
 - Whiskers - Normalizers
- Coming soon
 - Calvin – SIEM-tooling/Network monitoring
 - Otis – Signing tool



Al giorno d'oggi

#feedmehuman

I
CATNIP





Bevindingen

Een overzicht van alle bevindingen die OpenKAT heeft gevonden op . Elke bevinding heeft betrekking op een object. Klik op een bevinding voor meer informatie.

[Bevinding toevoegen](#)[Bevindingstype toevoegen](#)[Download PDF](#)[Filteropties tonen](#)

Toont 20 van 48 bevindingen

<input type="checkbox"/>	Niveau	Bevinding	Boom	Graaf	Details
<input type="checkbox"/>	Critical	KAT-NXDOMAIN-HEADER @ Content-Security-Policy @ http://mispo.es:80/ @ 134.209.85.72 contains asfsdgsrgew223424.com	🌳	🔗	⌵
<input type="checkbox"/>	Critical	KAT-CERTIFICATE-EXPIRED @ Let's Encrypt (00000481205130258951845928efc2281374ef13)	🌳	🔗	⌵
<input type="checkbox"/>	Medium	KAT-CSP-VULNERABILITIES @ Content-Security-Policy @ https://mispo.es:443/ @ 134.209.85.72	🌳	🔗	⌵
<input type="checkbox"/>	Medium	KAT-NO-HSTS @ https://mispo.es:443/ @ 134.209.85.72	🌳	🔗	⌵
<input type="checkbox"/>	Medium	KAT-NO-DKIM @ asfsdgsrgew223424.com	🌳	🔗	⌵
<input type="checkbox"/>	Medium	KAT-NO-DMARC @ asfsdgsrgew223424.com	🌳	🔗	⌵
<input type="checkbox"/>	Medium	KAT-NO-SPF @ asfsdgsrgew223424.com	🌳	🔗	⌵
<input type="checkbox"/>	Medium	KAT-NXDOMAIN @ asfsdgsrgew223424.com	🌳	🔗	⌵
<input type="checkbox"/>	Medium	KAT-NO-DMARC @ domaindiscount24.net	🌳	🔗	⌵



Kwetsbaarheden Analyse Tool



4-10-2021



KAT Kwetsbaarheden Analyse Tool

Futuro





De toekomst is compliance
NIS2 – CRA – DORA -

Omnino Consultants



Non compliant



Not pentested



Unknown risks
accepted

Approved for release





Opzet, bestaan en
werking

Uitgangspunt



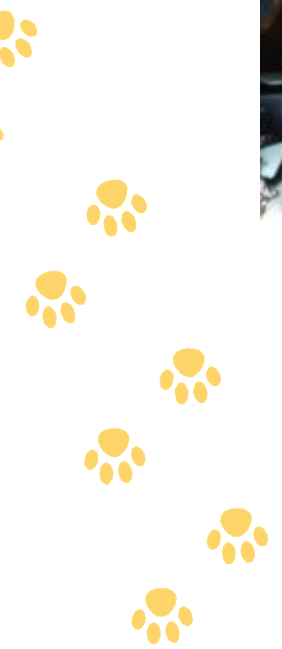
OPZET



BESTAAN



WERKING





as

Crisis Room KAT-atalogus Bevindingen Rapporten Objecten Taken Leden Instellingen

Nederlands

A

Rapporten > Choose report types > Set up scan > View Report



KAT Kwetsbaarheden Analyse Tool

Findings Report for organization as

Observed at: 4 oktober 2023 13:19

Created by: a

Samenvatting

Selected OOs

Object	Type	Vrijwaringsniveau
Hostname internet miso.es	Hostname	👍👍👍
IPService internet 134.209.85.72 tcp 443 https	IPService	👍👍👍
IPService internet 178.22.85.10 tcp 443 https	IPService	👍👍👍

Selected Report Types

Report type	Omschrijving
TLS Report	TLS reports assess the security of data encryption and transmission protocols.
DNS Rapport	DNS reports focus on domain name system configuration and potential weaknesses.

Selected Plugins for scans

Plug-in naam	Plugin scan level	Plug-in type	Plug-in beschrijving
Testssl.sh Ciphers	👍👍👍	Boefje	Run testssl.sh Docker container and check ciphers
Dnssec	👍👍👍	Boefje	Validates DNSSec of a hostname
DnsRecords	👍👍👍	Boefje	Fetch the DNS record(s) of a hostname

Other records found

Record	Waarde	Found by
miso.es MX 10 mx.wijmailenvellig.nl.	10 mx.wijmailenvellig.nl.	kat_dins_normalize
miso.es SOA ns1.domaindiscount24.net.	ns1.domaindiscount24.net. tech.keysystems.net. 2023012324 10800 3600 604800 3600	kat_dins_normalize

Security

Type	Ingeschakeld
SPF	False
DMARC	False
DKIM	False
DNSSEC	False

TLS Report for IPService|internet|134.209.85.72|tcp|443|https

Ciphers

Protocol	Naam	Encryption Algorithm	Bits	Key Size	Code	Bevinding
TLSv1.3	TLS_AES_256_GCM_SHA384	AESGCM	253	256	x1302	👍 Good
TLSv1.3	TLS_CHACHA20_POLY1305_SHA256	ChaCha20	253	256	x1303	👍 Good
TLSv1.3	TLS_AES_128_GCM_SHA256	AESGCM	253	128	x1301	👍 Good
TLSv1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	AESGCM	521	256	xc030	👍 Good
TLSv1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	AESGCM	2048	256	x9f	👍 Good
TLSv1.2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	ChaCha20	521	256	xcca8	👍 Good
TLSv1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	AESGCM	521	128	xc02f	👍 Good
TLSv1.2	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	AESGCM	2048	128	x9e	👍 Good

TLS Report for IPService|internet|178.22.85.10|tcp|443|https

Ciphers

Protocol	Naam	Encryption Algorithm	Bits	Key Size	Code	Bevinding
TLSv1.3	TLS_CHACHA20_POLY1305_SHA256	ChaCha20	253	256	x1303	👍 Good
TLSv1.3	TLS_AES_256_GCM_SHA384	AESGCM	253	256	x1302	👍 Good
TLSv1.3	TLS_AES_128_GCM_SHA256	AESGCM	253	128	x1301	👍 Good
TLSv1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	AESGCM	256	256	xc030	👍 Good
TLSv1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	AESGCM	256	128	xc02f	👍 Good
TLSv1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	AES	256	256	xc028	🚫 Phase out
TLSv1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	AES	256	128	xc027	🚫 Phase out

Findings

Ausiliari





Kittens

A close-up, low-angle shot of the character Zorro. He is wearing a dark, wide-brimmed hat and a dark coat with a high collar. His face is pale with a white muzzle, and he has striking yellow eyes. He is looking directly at the camera with a serious expression. The background is dark and out of focus, showing some architectural details and a small, warm light source on the right.

Zorro

Calvin: Hoog volume SIEM met Privacy-by-Design





Hoe het nu soms gaat

- Geef me alle logs en ik destilleer de use-cases
- Logboeken van jaren toegankelijk & vrij kneedbaar
- Geen sprake van Privacy-by-Design
- SIEM vaak ook onderzoekstool
- Gebrek aan functiescheiding
- Geen standaard in opslag

Monitoring veel gevraagd

- ISO 27001:2022 --> NEN7510
- WEGIZ
- NIS2





Meer data dan je eigenlijk aankunt

- Grote datastromen (logboeken en soms netwerkstromen)
- Meer dan je aan kunt
- Lastig schiften in relevante en minder relevante cases
- Ontbrekende context data



Gezondheidsgegevens

- Bijzondere persoonsgegevens
- „gegevens over gezondheid”: persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven;
- In principe verboden te verwerken
- Toegankelijk op een need to know voor zorgverleners



Toegang monitoring conform NEN7513

NEN 7513 is een Nederlandse norm die de logging van elektronische patiëntendossiers regelt. Het stelt eisen aan het loggen van acties op elektronische patiëntgegevens om de privacy van patiënten te waarborgen en ongeoorloofde toegang tot of manipulatie van deze gegevens te detecteren.

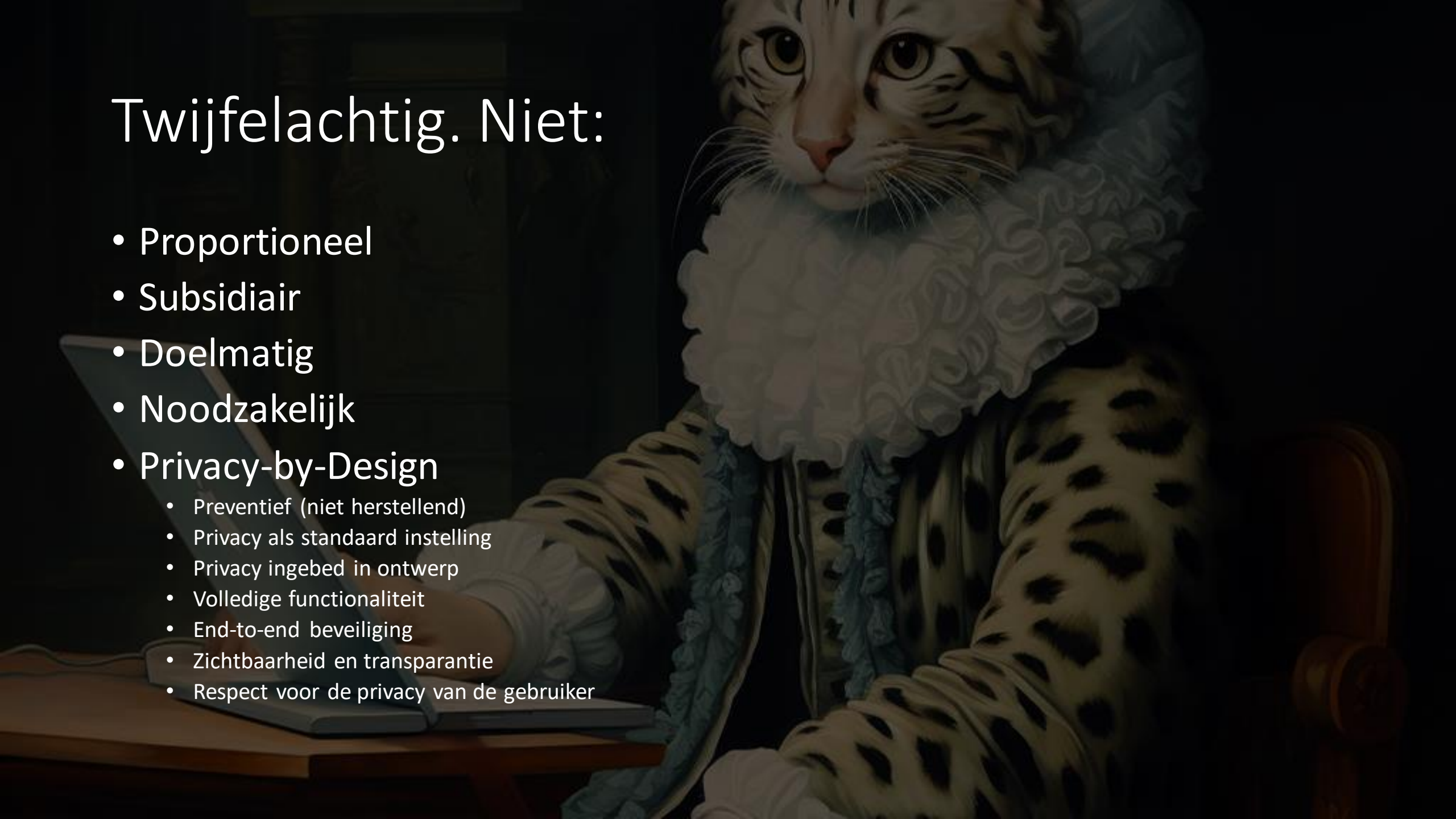
Gevolg

- Logboek bevat opnieuw gezondheidsgegevens
- Valt veel uit af te leiden
- SOC-medewerkers doorgaans niet BIG-geregistreerd
- Medewerkers gebruiken doorgaans alle logboekgegevens om use cases te maken



Twijfelachtig. Niet:

- Proportioneel
- Subsidiair
- Doelmatig
- Noodzakelijk
- Privacy-by-Design
 - Preventief (niet herstellend)
 - Privacy als standaard instelling
 - Privacy ingebed in ontwerp
 - Volledige functionaliteit
 - End-to-end beveiliging
 - Zichtbaarheid en transparantie
 - Respect voor de privacy van de gebruiker



Maak logboeken querybaar

- Bestaande oplossing
- Grote volumes data
- Focus horizontaal en verticaal
- Microservice architectuur
- Patroon herkenning





Aufenthaltsliste vom 25.02.2020

Name	Adresse	Uhrzeit von/bis
M. Fiedler	Krausstr. 11	12:20
Paula	Polakstr. 11	10:30
Liam		12:45
G. Schmeißinger	Fleischerei	19:30
Unone		13:15
Gabine Paulowk.		12:30
Waller		14:00 - 16:50
Nils + Dani	UNAST	14:00
Regine		14:00
Lo Dietz		15:00
Fam. Stock		15:00
Kennib		12:00
Puig		12:00
Kiow		16:00

Logboeken

- Toon alleen dat wat relevant is
- De rest is niet zichtbaar

Simpel proces

Denk use case uit

- Kennis van systeem
- Standaard cases
- Op basis van voorgenomen functionaliteit

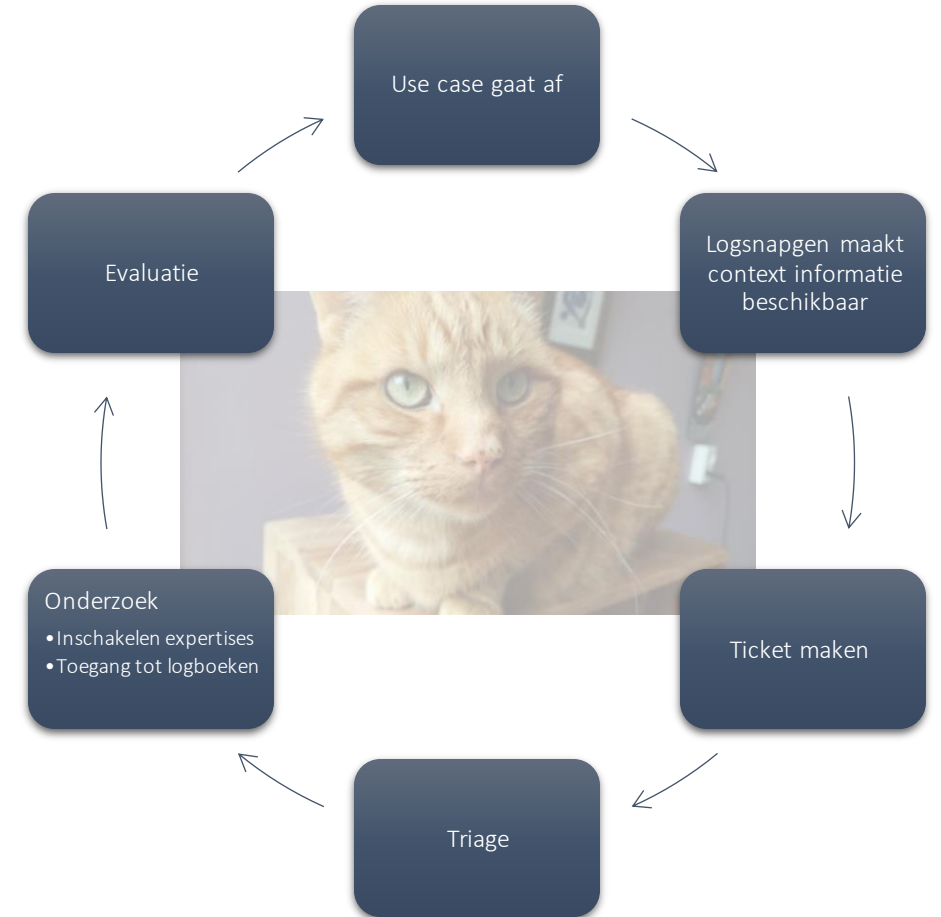
In productie

Bedenk nodige context data

Beoordeling privacyteam

Goedkeuring of gebouwd is wat is toetsaan

Bouw use case



Evaluatie

Use case gaat af

Logsnapgen maakt context informatie beschikbaar

Onderzoek

- Inschakelen expertises
- Toegang tot logboeken

Ticket maken

Triage



Calvin

- Apache-Kafka
- RabbitMQ
- KSQL-use cases
- Doel data aanleveren aan ticketsysteem en OpenKAT

Calvin privacy vriendelijke loganalyse



LOGREGELS

Activiteiten wordt gelogd
Logregels worden opgeslagen in een logfile
Logtail pakt de nieuwste logregels op

Calvin analyseert logs aan de hand van usecases

AUTOMATISCHE ANALYSE

Voorbeelden usecases:
• 5 x inloggen zonder wachtwoord
• >2000 toetsenbordaanslagen per minuut
• verdachte IP-range



TRIGGERT INCIDENT

Incidenten gaan naar de outbox
Logregels + usecase + relevante context
Logregels worden opgeslagen

Onderzoeker beoordeelt incidentmelding:

1. Onschuldige situatie
2. Inzet technische ondersteuning
3. Start onderzoek



Privacyvriendelijk
in control





We are open! Doe mee!

- [Openkat.nl](https://www.openkat.nl)
- meedoen@openkat.nl

- Brenno de Winter
 - +31653536508
 - brenno@dewinter.com of dewinter@bren.no
 - X: [@brenno](https://twitter.com/brenno)

There is one more
thing!





C'è ancora una **cosa**

Vragen?

Bijvoorbeeld

- Hoe ga je om met standaarden met gedeeltelijk dezelfde controls?
- Wat doe je op dit moment met AI?
- Sommige controls bestaat alleen uit documentatie. Hoe ga je daarmee om?
- Gaat Keiko wel eens op vakantie?
- Waar staat OpenKAT over 10 jaar?
- Waarom heb je een slide met comic sans?
- Wordt de auditor nu overbodig?

