Ik zie, ik zie, wat jij niet ziet

Brenno de Winter
brenno@dewinter.com
06-53536508

Pandemie + Security != Kattenpis

Brenno de Winter, CSPO

Ministerie van Volksgezondheid, Welzijn en Sport

Het kabinet zet in op apps om de verspreiding van het coronavirus in te dammen. Dat bleek uit de woorden van minister De Jonge van Volksgezondheid op een persconferentie met premier Rutte over de bestrijding van het virus. "Twee apps vormen straks de kern van het nieuwe testbeleid", zei De Jonge, maar hij benadrukte dat er nog wel onderzoek wordt gedaan. "Alleen als de privacy gewaarborgd is, gaan we dit doen."

Het kabinet volgt de aanbevelingen van het Outbreak Management Team (OMT) van het RIVM. In een advies aan het kabinet, dat vandaag uitlekte via de NOS, stond ook al dat er onderzoek moet worden gedaan naar de inzet van mobiele applicaties. In landen als Zuid-Korea en Singapore wordt die technologie al gebruikt.

6 april 2020

Dodelijke cocktail

Een van de critici is Brenno de Winter. “Er is een totaal chaotisch proces doorlopen. Bizar dat apps uiteindelijk wel op de lijst terechtkomen, als je iets afwijst in een selectieprocedure. Het ministerie zegt: ‘We luisteren naar de experts.’ En dan doen ze het niet.”

Zo lijkt het volgens De Winter alsof die fase van het proces niets heeft voorgesteld. “Daarnaast geeft het ministerie nu alle signalen af dat dit project aan het mislukken is. Men gaat te snel. Men wil te veel. Men weet eigenlijk niet precies wat ze willen. Die eisen worden continu aangepast. Dat is een dodelijke cocktail voor ieder succesvol ICT-project.”

Lees ook: Kabinet: gebruik van corona-a

Het kabinet wil zo snel mogelijk twee wer
weekend werden app-ontwikkelaars en b
om twee apps: een contact-app die laat zi
gebruiker die besmet blijkt te zijn, en één
te houden met de dokter. De voorstellen
verbeterd worden, betreffen de contact-a

Nee ze fixten het niet

Je moet het zelf doen

Stuurman aan boord
Of
Aan wal?

Als je het zo goed weet … doe het zelf

NRC @nrc · Sep 9

Het maximale is gedaan om de **CoronaMelder** veilig te maken, zegt ‘privacy- en securitynerd’ Brenno de Winter. „Dit is next level.”

Reinier Ladan @Reinier · 22h

Leuk nieuwtje: ik ben sinds maandag aan de slag als product manager van de **CoronaMelder** app en ga binnen een paar weken @rickpastoor helemaal vervangen. Erg veel zin in dit mooie project!

Download die app

Dick Blaauw · 1st

Servicemanager AppLoket bij DICTU

Groningen Area, Netherlands · 500+ connections · Contact info

Dirk-Willem van Gulik

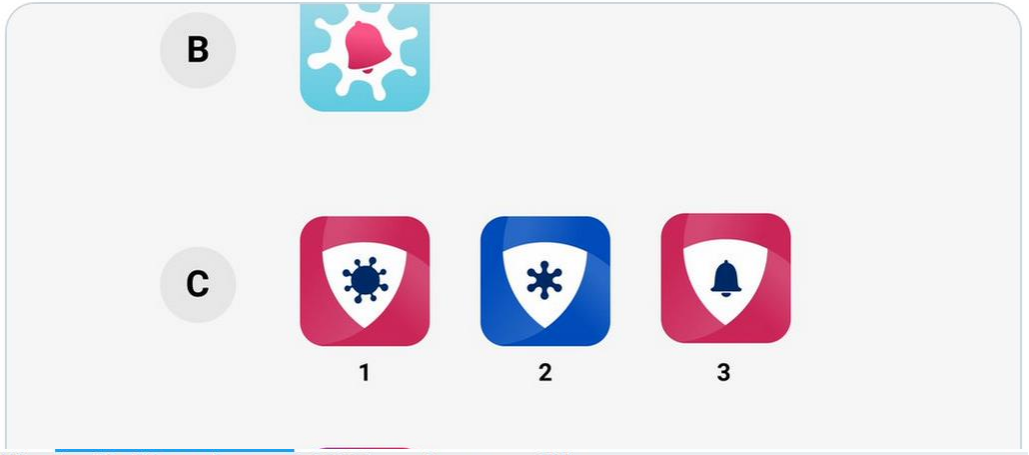
Vertaald uit het Engels - Dirk-Willem van Gulik is oprichter van de Apache Software Foundation en draagt bij aan het Apache Webserver-project. Van Gulik is de voormalige CTO van Joost, waar hij werd ontslagen, en de huidige Chief Technical Architect van British Broadcasting Corporation's Future Media and Technology.
Wikipedia (Engels)

Originele beschrijving bekijken

Jelle Prins @jelleprins · Jul 8

👋 📱 Welk icoon voor de Corona Melder app?

(zie thread voor poll & meer details)



Elisabeth Steenhoven @ESteenhoven · 19h

Over **#Coronamelder**

de begeleidingscommissie heeft het werk van de app-bouwers /@MinVWS zeker niet vereenvoudigd-integendeel.

Maar ere wie ere toekomt:

🚀 @Ron_Roozendaal voor Open Source proces

🚀 bouwers voor
— Privacy
— Backend
— Veiligheid

coronamelder.nl

Dreigingsniveau: statelijke actor

Dreigingsniveau statelijke actor	Zeer vocale activisten	APT realistisch	Veel incidenten internationaal
Negatief sentiment	Politiek zeer sensitief	Publiek zeer veel aandacht	Breed gedragen wantrouwen
	Matige kwaliteit onderzoek	Bredere kennis nodig	

Conclusie: doe wat echt juist is

- Transparant werken
- Leg de lat zo hoog mogelijk
- Borg de beveiliging
- Borg de privacy
- Voor iedereen toegankelijk
- Voor burgers betrouwbaar
- Maak het open (source)

Iedereen mocht meebouwen aan de CoronaMelder

Open source Technisch gezien is de CoronaMelder nagenoeg af. De ontwikkeling van deze corona-app was voor het eerst open source. Hoe verliep dat?

Rik Wassens 29 juli 2020 Leestijd 5 minuten

Van Putten kijkt uit naar het volgende grote opensourceproject van de overheid. „Als alles open source is, hou je er een beter controleerbare overheid aan over. Het zou mooi zijn als het nog eens kan, met een project dat onder niet zo'n hoge druk staat."

Fouten zijn tof

- Mensen maken fouten dus werk daarmee
  - Ontwerp robuust
  - Wees scherp op kwaliteit
  - Wees niet bang om fouten onder ogen te zien
- Geen reguliere risicoinschatting maar FMEA's

Pentest hoofdpijn

NOS Nieuws Sport Uitzendingen

NOS NIEUWS • BINNENLAND • TECH • 06-06-2020, 16:04 • AANGEPAST 06-06-2020, 18:29

Lek in RIVM-coronasite: gegevens van gebruikers makkelijk in te zien

Joost Schellevis
redacteur Tech

De site Infectieradar, waar Nederlanders kunnen doorgeven of ze de afgelopen week coronaklachten hebben gehad, bevatte een ernstig datalek. Iedereen met enige technische vaardigheid kon tot vanmorgen zien wat andere deelnemers antwoordden op persoonlijke en medische vragen.

SECURITY

Ophef over pentest bij gemeente Hof van Twente

IT-dienstverlener en pentester zouden zaken niet op orde hebben.

SECURITY

Hoe grondig is de vereiste pentest voor coronatestbedrijven?

Lek in Testcoronanu had met pentest gevonden moeten worden, maar dat gebeurde niet.

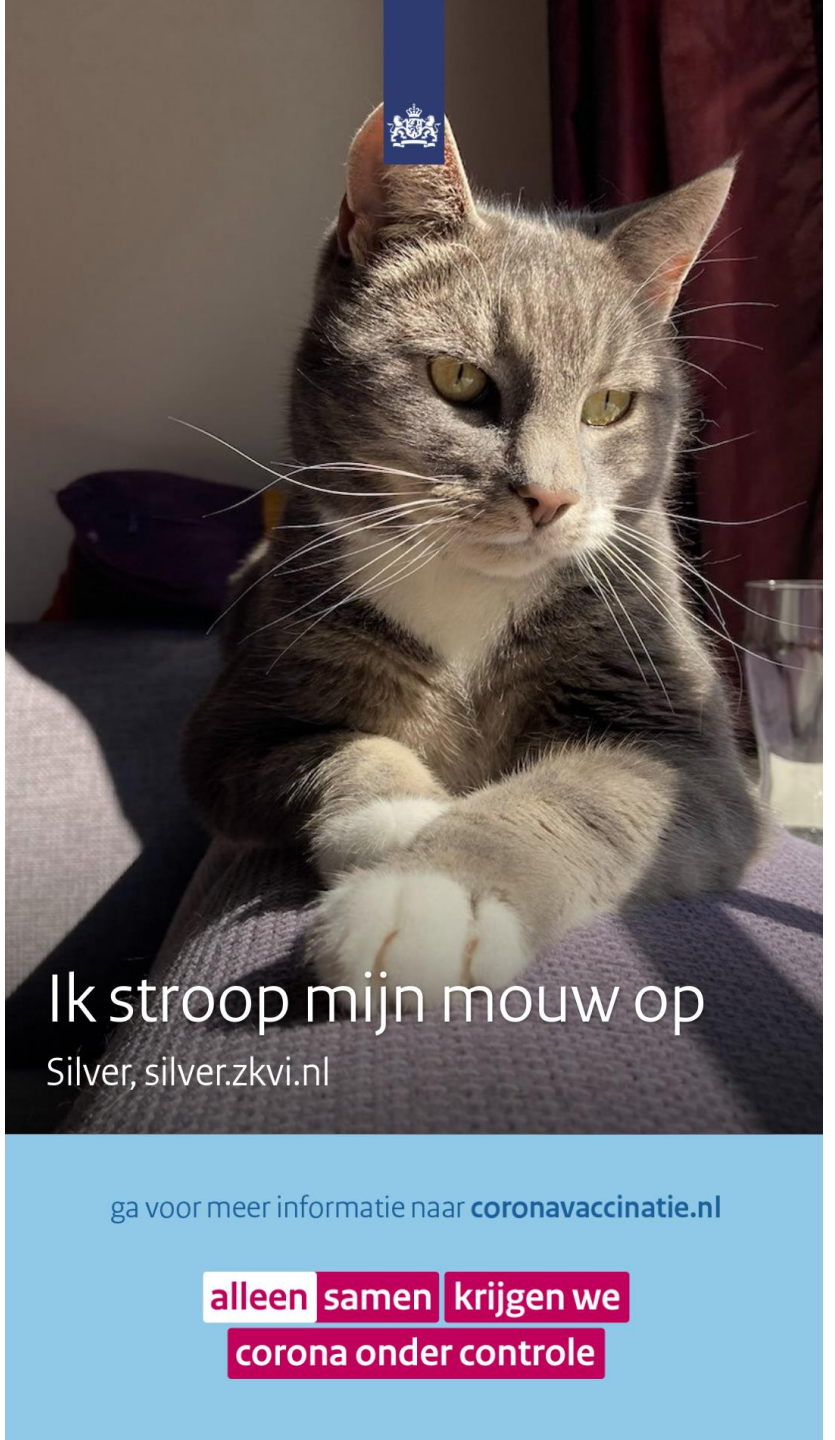
Bedrijfsauto's zwaar | Driewielige motorrijtuigen | Aanhangwagens | Landbou bosbouw

Inkoopeisen

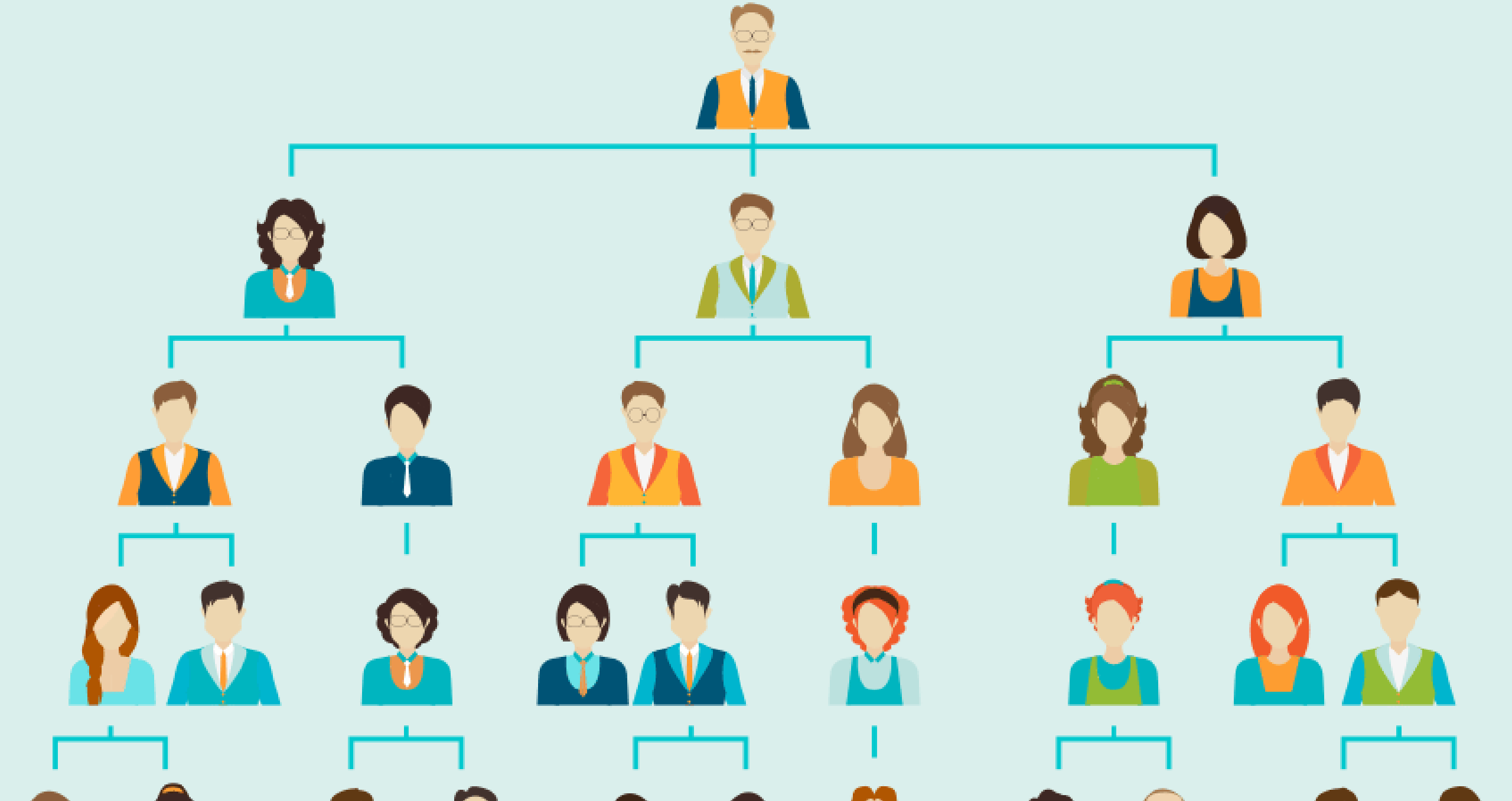
- Uniforme eisen voor inkoop van pentesten
- Alle bevindingen langs dezelfde meetlat (CVSS)
- Een minimale set aan eisen:
  - OWASP TOP-10
  - MSTG/WSTG
- Uniforme manier van presenteren van bevindingen: PTES
- Reproduceerbaarheid van het onderzoek
- Het rapport wordt openbaar

Als er vaccins komen....

Ehh …. hoe registreren we dat?




BLAH
BLAH
BLAH
BLAH



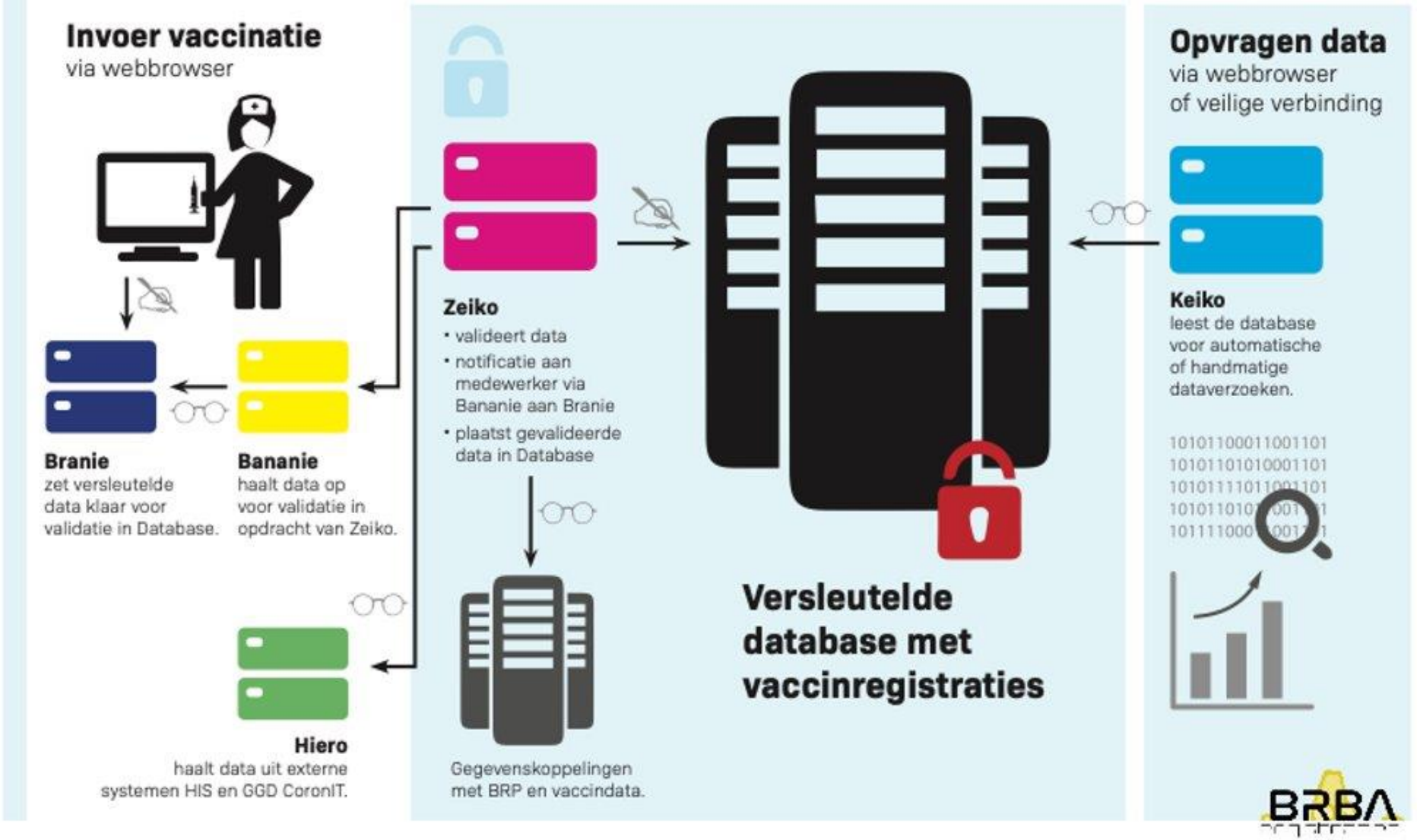
Nee ze fixten het niet

Je moet het zelf doen


Binnenkort opent hier BranieBananie
De webshop voor al uw bananen
BRANIE BANANI

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

Rijksoverheid



BRBA


VPN-CLT-05
ProLiant DL20 Gen10
utimaco®
Host1
Host2
HSM
HSM-BRBA-01
- CryptoServer LAN -
HSM Battery
Voltage: 3.073 V
OK
Erase
utimaco®
Host1
Host2
HSM
HSM-BRBA-03
- CryptoServer LAN -
HSM Battery
Voltage: 3.066 V
OK
Erase
utimaco®
Host1
Host2
HSM
HSM-BRBA-05
- CryptoServer LAN -
CSLAN Status
Connections: 0
Trans./min.: 0
Erase

HSM on a Yubikey

Uitrol naar ziekenhuizen

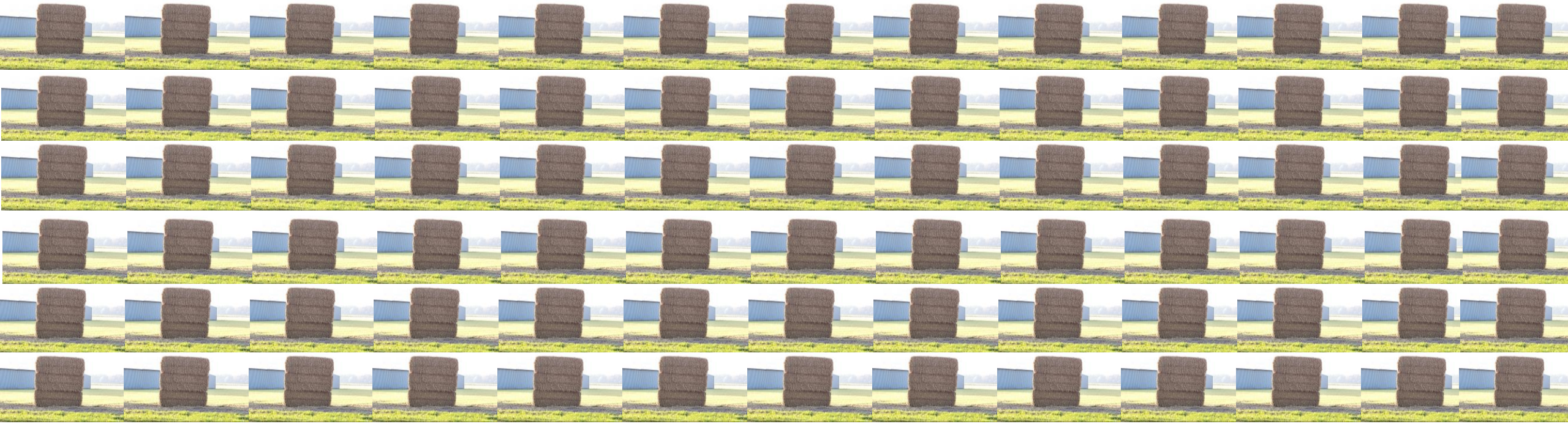
Inloggen met een UZI-pas

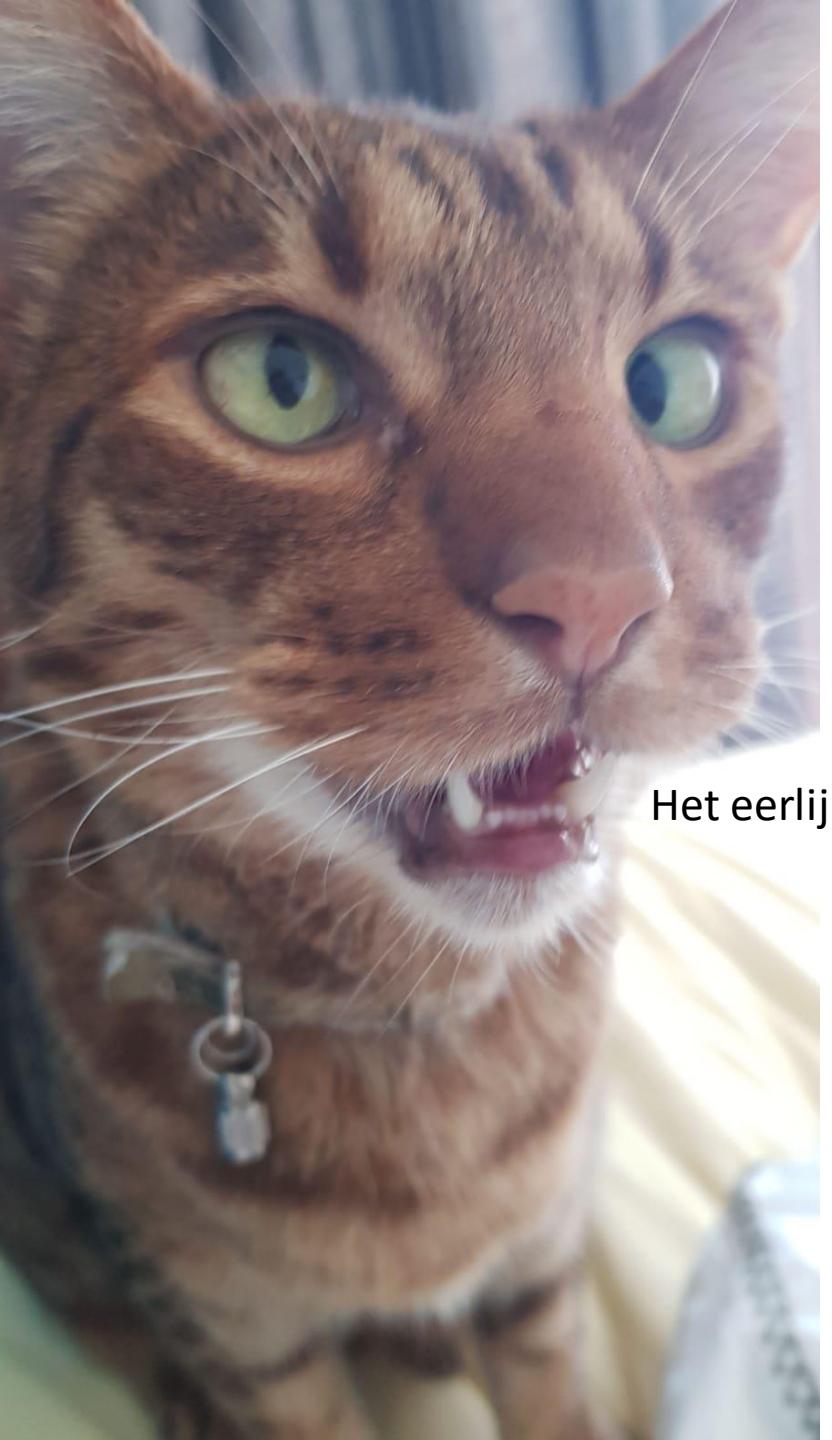
Verder nog veel te bewaken

- Pentesten
- Codereviews
- Domeinbewaking
- Bewaking app stores
- Risicoanalyses (FMEA)
- Compliance monitoring
- Bewaking configuraties
- Fraude met QR-codes
- DDoS
- Alles bewijsbaar en uitlegbaar

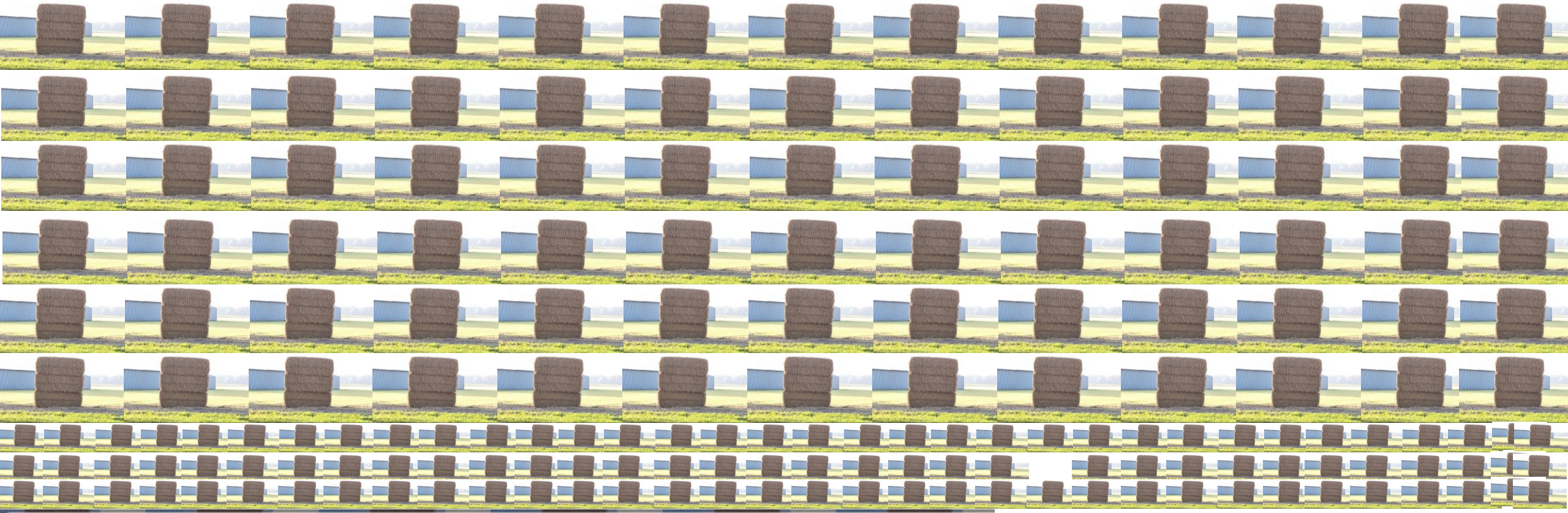
Is goed gaan we doen – ehh Brenno hou jij de boel in de gaten?

- CoronaMelder
- GGD Contact (bron- en contactonderzoek)
- Braniebananie (BRBA) - vaccinatiedoorgifte
- Ondersteuning bij GGD (Red Teaming)
- CoronaCheck – Corona toegangsbewijs
- Stelselbewaking CoronaCheck - testaanbieders
- ZKVI – Vaccinatie EPD voor ziekenhuizen
- DCC – Europees Coronabewijs
- CKVI – DCC regelen voor bellers
- HKVI – Voor huisartsen
- GKVI – DCC uitgifte voor uitzonderingen GGD
- KVTB – Toeristenroute voor CTB
- UZIPOC
- Begeleid Zelf testen
- Abonnementsdienst voor uitzonderingsroutes
- Screening voor toegang tot BRBA, HKVI
- Fraudebestrijding rond QR-codes
- Curacao
- Aruba
- Sint Maarten





Het eerlijke verhaal Brenno!



Microsoft PowerPoint

We kunnen niets anders invoegen op de dia 25 omdat de webversie van PowerPoint alleen 200 items op een dia kan bevatten. U kunt dit bestand echter openen in Microsoft PowerPoint om meer items op de dia in te voegen.

Uw feedback helpt Microsoft om PowerPoint te verbeteren.
Geef feedback aan Microsoft

OK

Ofwel

- 20 projecten
- Plm. 40 testaanbieders
- ~~150~~ ~~1.500~~ 3.600 domeinen van VWS
- En op termijn meer zorgaanbieders

Hoe bewaak je dat?

Regelen anderen dat voor je?

Nee ze fixten het niet

Je moet het zelf doen

Realisatie 1: Bijna alle incidenten vloeien voort uit basale fouten

- Veel berust op gebrekkige basis maatregelen
- Veel berust op configuratiefouten
- Veel berust op systemen die onbekend zijn
- Veel berust op niet bijhouden van de softwarestack

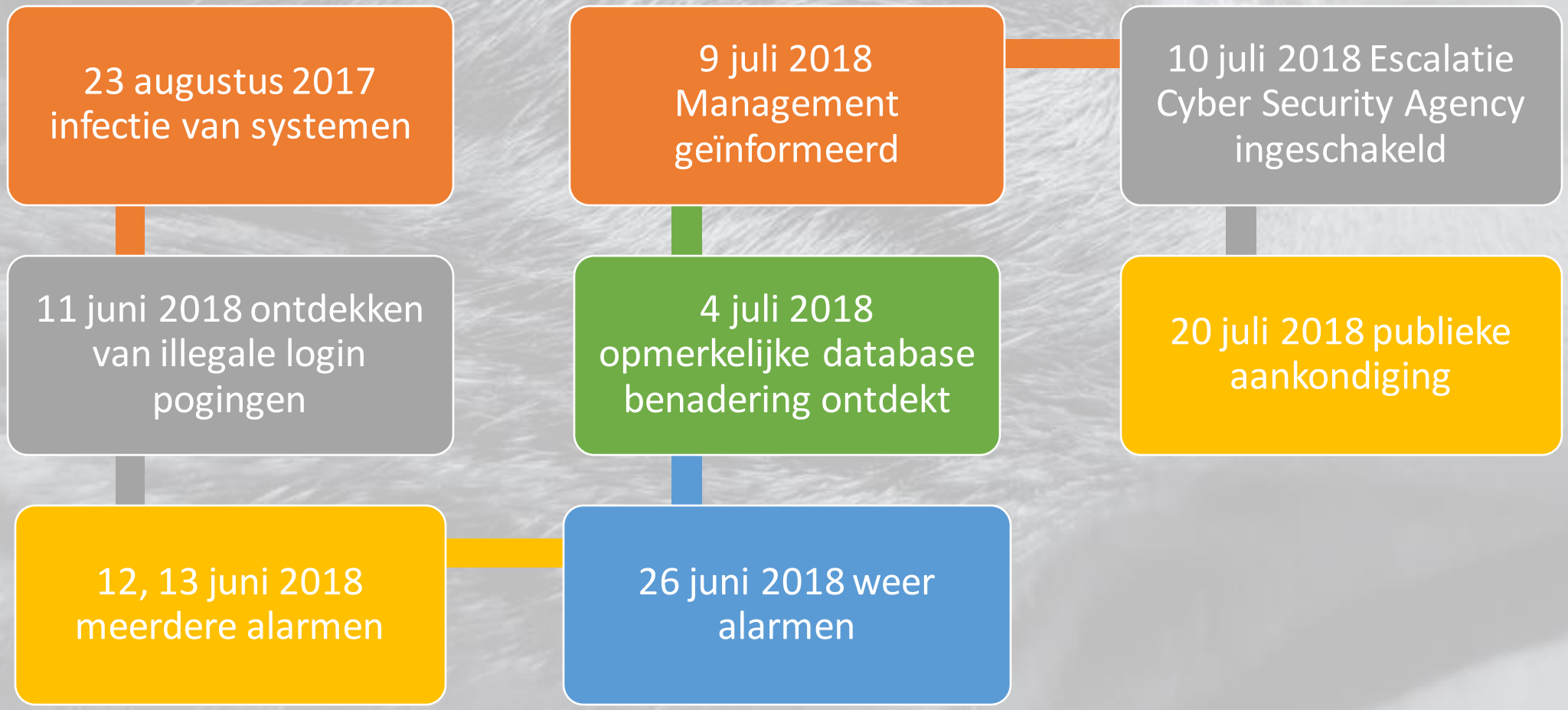
```
Certificate:  Data:     Version: 3 (0x2)
Serial Number:
05:e2:e6:a4:cd:09:ea:54:d6:65:b0:75:fe:22:a2:56
Signature Algorithm: sha1WithRSAEncryption
Issuer:
emailAddress                = info@diginotar.nl
commonName                  = DigiNotar Public CA 2025
organizationName            = DigiNotar
countryName                 = NL
Validity Not Before: Jul 10 19:06:30 2011 GMT
Not After : Jul  9 19:06:30 2013 GMT
commonName                  = *.google.com
serialNumber                = PK000229200002
localityName                = Mountain View
organizationName            = Google Inc
countryName                 = US
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (2048 bit)
```

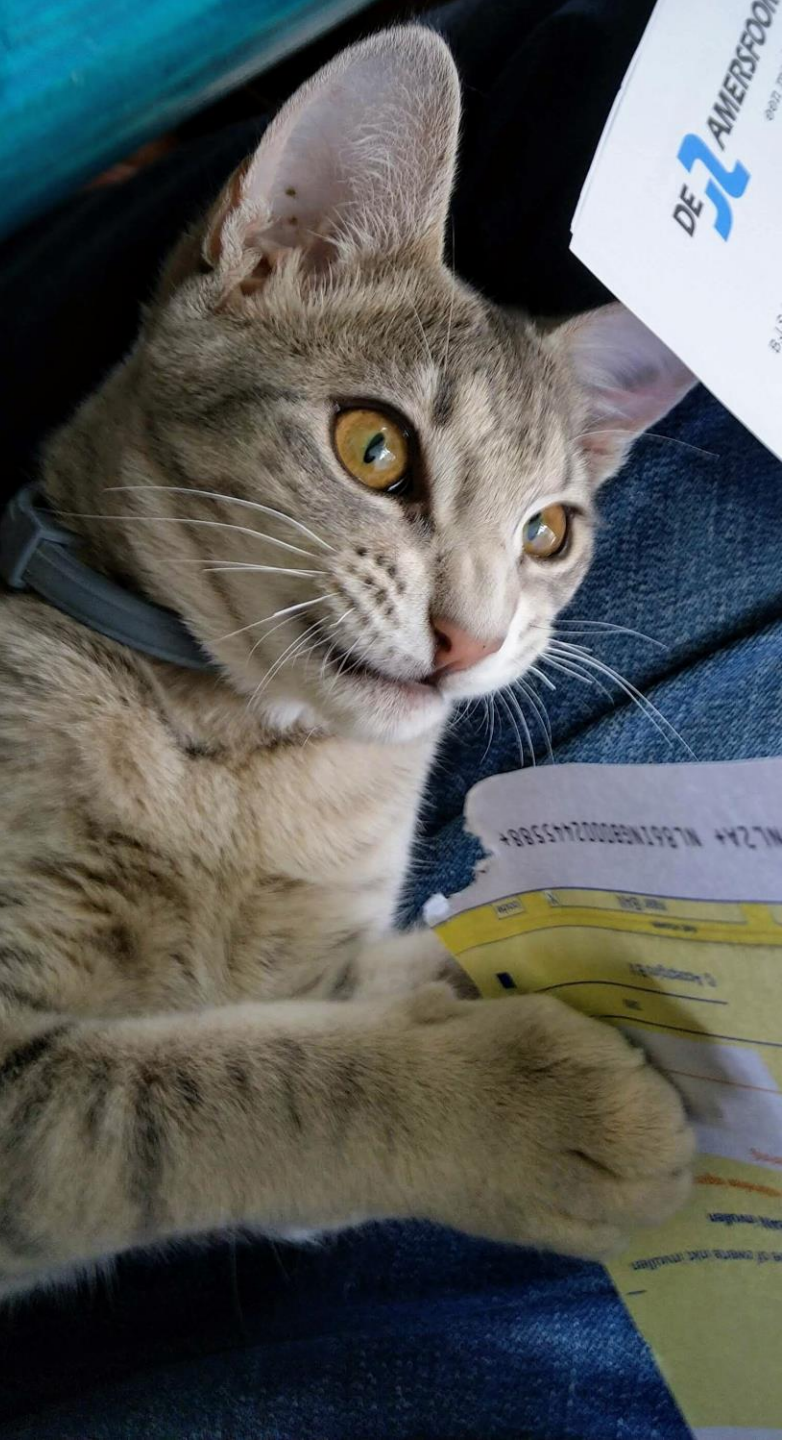

PRESS ANY KEY!


kpn


What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
bitcoin
Send $300 worth of bitcoin to this address:

Zorgadministratie Singapore





De hack op de Democratische Partij

- Aanval uitgevoerd met simpele phishing email
- Na klikken usernaam/wachtwoord invullen
- Toegang tot alle e-mailberichten
- Openbaarmaking via Wikileaks

Het is geen wapenwedloop

Lochem

- Geen meerfactorauthenticatie
- Verouderde software
- Onbekende systemen
- Beheer dat tekort schiet

Hof van Twente

- Geen meerfactorauthenticatie
- Slechte wachtwoorden
- Verouderde software
- Beheer dat tekort schiet

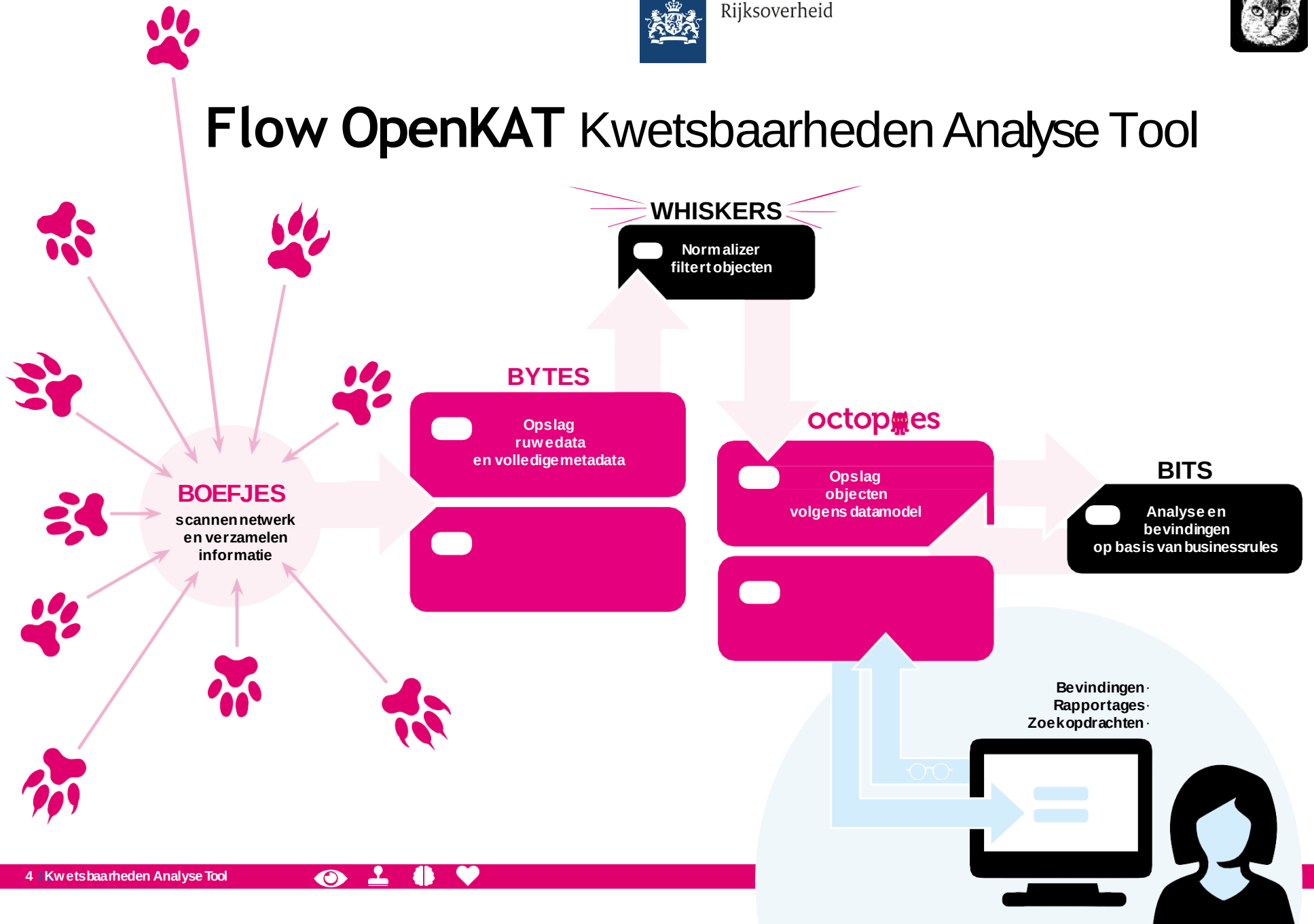
Realisatie 2:
Security Operations

- Gaat niet over alleen lopende aanvallen
- Gaat juist om compliance
- Gaat over kwaliteit
- Gaat juist over lifecycle
- Gaat over alles waar je over kwetsbaarheden spreekt
- Continu proces

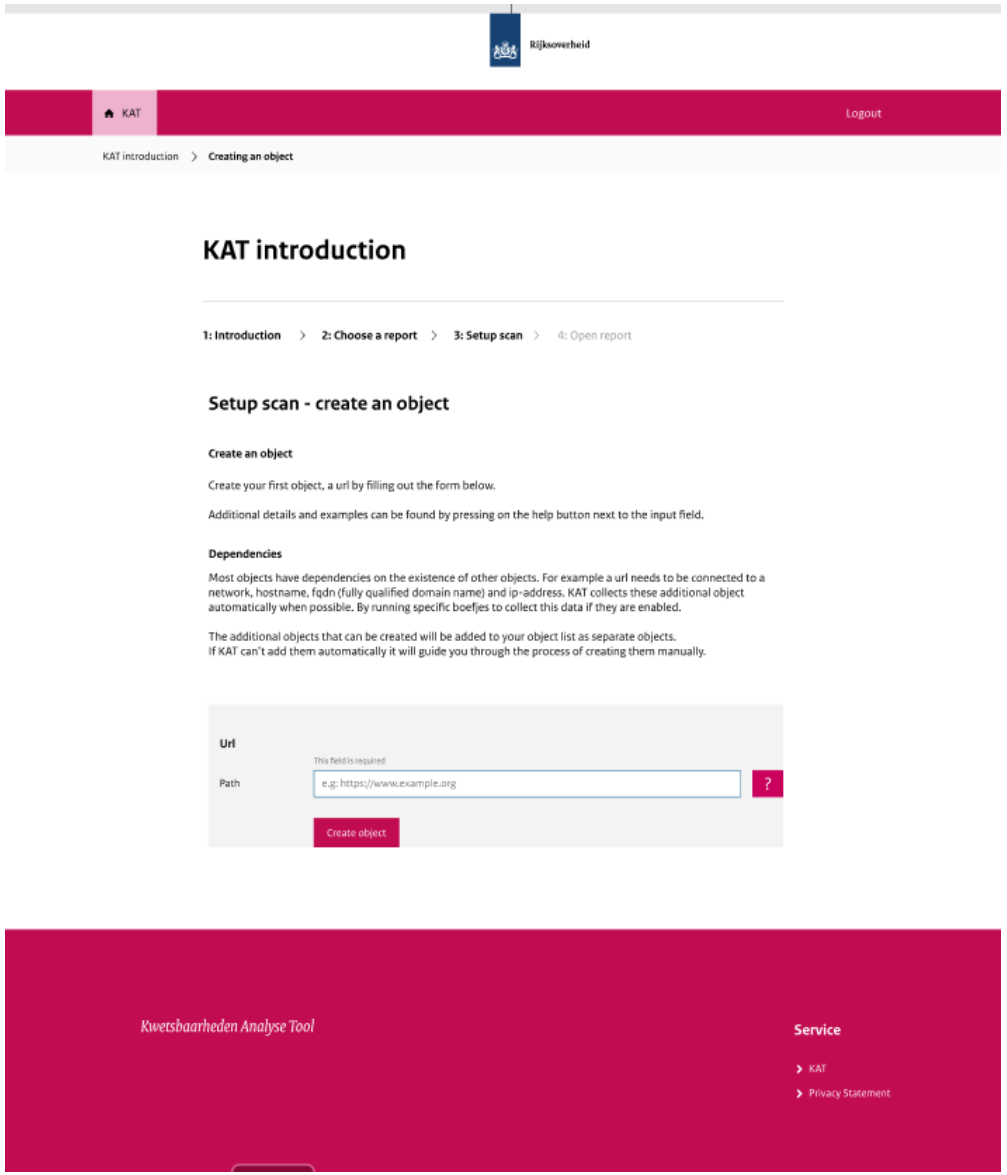
Realisatie 3: Ken je data

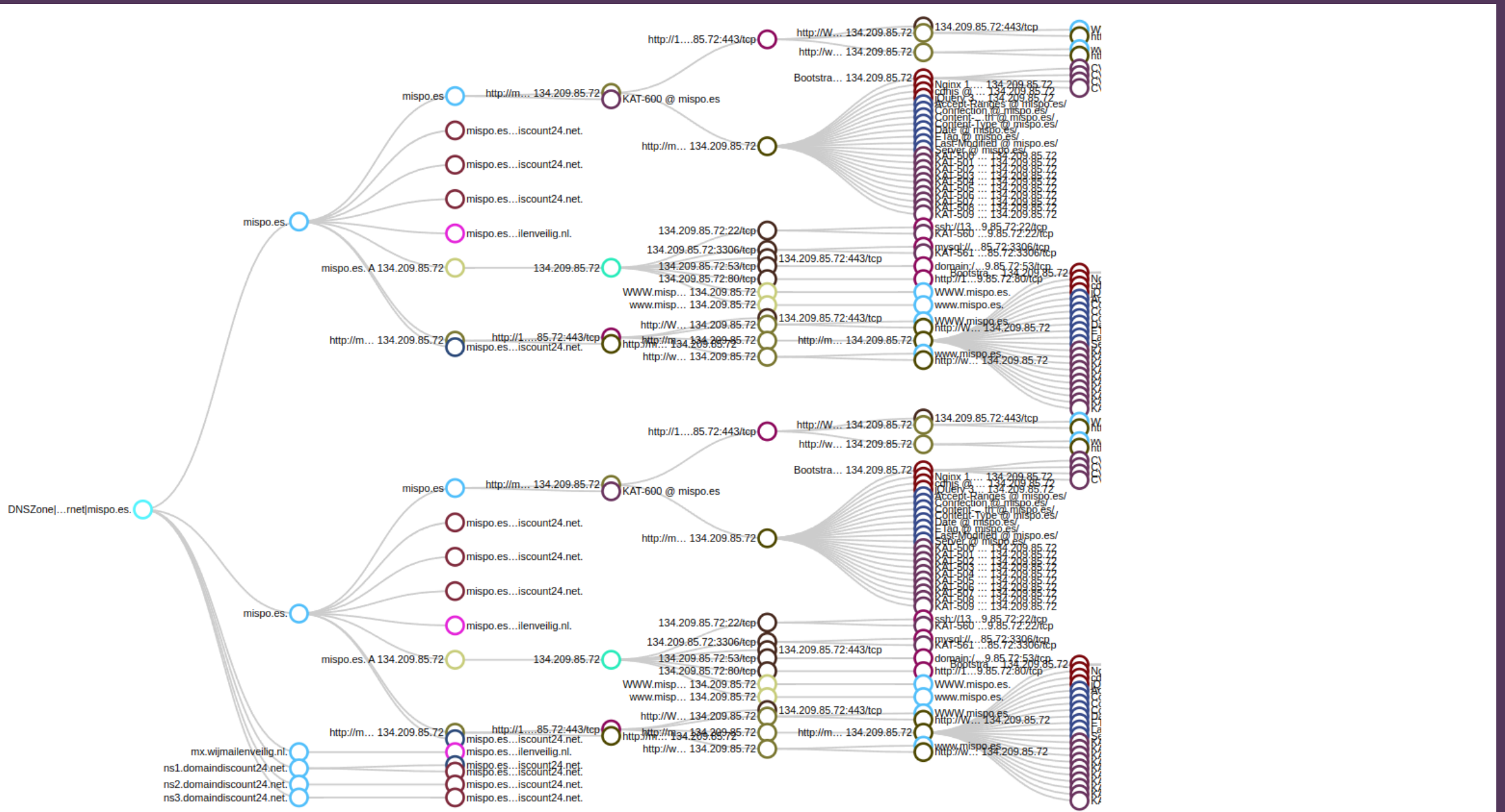
- Geen kale bak met ongestructureerde data
- Boefjes halen data op
  - API's
  - Externe bronnen
  - Tools
- Whiskers herkennen objecten en plaatsen het in de database
- Dus stro bij stro en spelden bij spelden

Flow OpenKAT Kwetsbaarheden Analyse Tool




Tim Abang


Rijksoverheid
KAT
Logout
KAT introduction
Creating an object
KAT introduction
1: Introduction
2: Choose a report
3: Setup scan
4: Open report
Setup scan - create an object
Create an object
Create your first object, a url by filling out the form below.
Additional details and examples can be found by pressing on the help button next to the input field.
Dependencies
Most objects have dependencies on the existence of other objects. For example a url needs to be connected to a network, hostname, fqdn (fully qualified domain name) and ip-address. KAT collects these additional object automatically when possible. By running specific boefjes to collect this data if they are enabled.
The additional objects that can be created will be added to your object list as separate objects.
If KAT can't add them automatically it will guide you through the process of creating them manually.
Url
This field is required
Path
e.g: https://www.example.org
?
Create object
Kwetsbaarheden Analyse Tool
Service
KAT
Privacy Statement


DNSZone|…rnet|mispo.es.
mispo.es.
mispo.es
mispo.es…iscount24.net.
mispo.es…iscount24.net.
mispo.es…iscount24.net.
mispo.es…ilenveilig.nl.
mispo.es. A 134.209.85.72
134.209.85.72
http://m… 134.209.85.72
http://1….85.72:443/tcp
mispo.es…iscount24.net.
http://m… 134.209.85.72
KAT-600 @ mispo.es
http://1….85.72:443/tcp
http://m… 134.209.85.72
http://W… 134.209.85.72
http://w… 134.209.85.72
134.209.85.72:443/tcp
Bootstra… 134.209.85.72
Nginx 1… 134.209.85.72
cdnis @… 134.209.85.72
jQuery-3… 134.209.85.72
Accept-Ranges @ mispo.es/
Connection @ mispo.es/
Content-… tf @ mispo.es/
Content-Type @ mispo.es/
Date @ mispo.es/
ETag @ mispo.es/
Last-Modified @ mispo.es/
Server @ mispo.es/
KAT-500 … 134.209.85.72
KAT-501 … 134.209.85.72
KAT-502 … 134.209.85.72
KAT-503 … 134.209.85.72
KAT-504 … 134.209.85.72
KAT-505 … 134.209.85.72
KAT-506 … 134.209.85.72
KAT-507 … 134.209.85.72
KAT-508 … 134.209.85.72
KAT-509 … 134.209.85.72
134.209.85.72:22/tcp
134.209.85.72:3306/tcp
134.209.85.72:53/tcp
134.209.85.72:80/tcp
WWW.misp… 134.209.85.72
www.misp… 134.209.85.72
http://W… 134.209.85.72
http://m… 134.209.85.72
http://w… 134.209.85.72
134.209.85.72:443/tcp
ssh://13…9.85.72:22/tcp
KAT-560 …9.85.72:22/tcp
mysql://…85.72:3306/tcp
KAT-561 …85.72:3306/tcp
domain:/…9.85.72:53/tcp
Bootstra… 134.209.85.72
http://1…9.85.72:80/tcp
WWW.mispo.es.
www.mispo.es.
WWW.mispo.es.
http://W… 134.209.85.72
www.mispo.es.
http://w… 134.209.85.72
mx.wijmailenveilig.nl.
ns1.domaindiscount24.net.
ns2.domaindiscount24.net.
ns3.domaindiscount24.net.

Realisatie 4: Scheiden feiten en conclusies

- We slaan een kopie van de werkelijkheid op
- We detecteren veranderingen in de database
- Op basis van business rules worden conclusies getrokken

Findings

11 Findings on example.org

Show filter options

Findings for website https://example-com on 4th of March 2021:

Risk level	Finding type	Occurrences	First known occurence	Status	Details
Critical	Cat has access to passwords	1	March. 4, 2021 5:30pm	New	
Critical	Cat tweeted the passwords	9001	March. 4, 2021 5:30pm	New	
High	Kittens inside the database	12	March. 4, 2021 5:30pm	New	
High	Outdated third party software used	2	March. 4, 2021 5:30pm	New	
High	Inline javascript	15	March. 4, 2021 5:30pm	New	
Medium	Session cookie is valid for too long	1	March. 4, 2021 5:30pm	New	
Medium	Initial administrator password decryptable available in the database	1	Feb. 15, 2021 2:45pm	Known	
Medium	Missing anti-hijacking security measures	1	Feb. 15, 2021 2:45pm	Known	
Low	Incomplete auditlog	1	March. 4, 2021 5:30pm	New	
Low	No automatic referral to https	1	March. 4, 2021 5:30pm	New	
Informational	2-factor authentication currently not required	1	March. 4, 2021 5:30pm	New	

Realisatie 5: Security is context gedreven

- Bij bevindingen geven we context
  - Wat zien we?
  - Waarom vinden we daar wat van?
  - Hoe neem je de bevinding weg?
  - We kijken naar de omgeving
- Bevindingen relateren we aan risico's

Risk level	Finding type	Occurrences	Status
Critical	Cat has access to passwords	1	New

Finding id: 1

Finding details

Finding: Cat has access to passwords

Description: Cat has free access to passwords Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean lobortis enim ac sapien lobortis, vitae congue odio scelerisque. Morbi orci purus, tristique sed ullamcorper sed, efficitur quis enim.

Risk level: 10/10

Impact: Giving a cat free access to passwords is a high security risk due to the unpredictable and often destructive nature of cats. Research has shown that giving cats free access to passwords often results in data leaks [source: https://examplesite.com].

Occurrences

Total occurences: 9001

Occurence: **https://example.nl/account/secret/catstash**

Time of testing: 04-03-2021 12:15

Proof: [..] Set-Cookie: csrftoken=httiJeEYjYZoBU6Ibom4N0MfgRX46RnU rCdsjqOgg6Kxr0RbMNRoqUG6s2wwuVGN; expires=Tue, 22 Feb 2022 20:50:53 GMT; Max-Age=31449600; Path=/; SameSite=Strict; Secure [..]

Reproduction: GET /account/login/ HTTP/1.1 Host: keiko.braniebananie.nl

Exporteer

?

Realisatie 6: Doe niet handmatig wat je kunt automatiseren

- Alles wat we kunnen weg automatiseren, automatiseren we weg
- Alles wat niet te automatiseren is, laten we met rust
- We ondersteunen de medewerker wel

Pen Test Report example.org

March. 4, 2021 5:30

These are the findings of a KAT-analysis on the 4th of March 2021. Click a finding for more detailed information about the issue, its origin, severity and possible solutions.

Vivamus congue rutrum turpis sit amet suscipit. Integer cursus auctor ex, sit amet vulputate turpis ornare nec. In sit amet neque sit amet elit interdum placerat quis at sapien. Phasellus molestie dignissim neque ut hendrerit. In maximus gravida metus quis blandit. Proin dignissim condimentum urna molestie ornare. Praesent dapibus, risus id euismod dictum, nisl libero vulputate metus, a elementum leo velit quis odio. Duis id sagittis ligula.

Number of findings

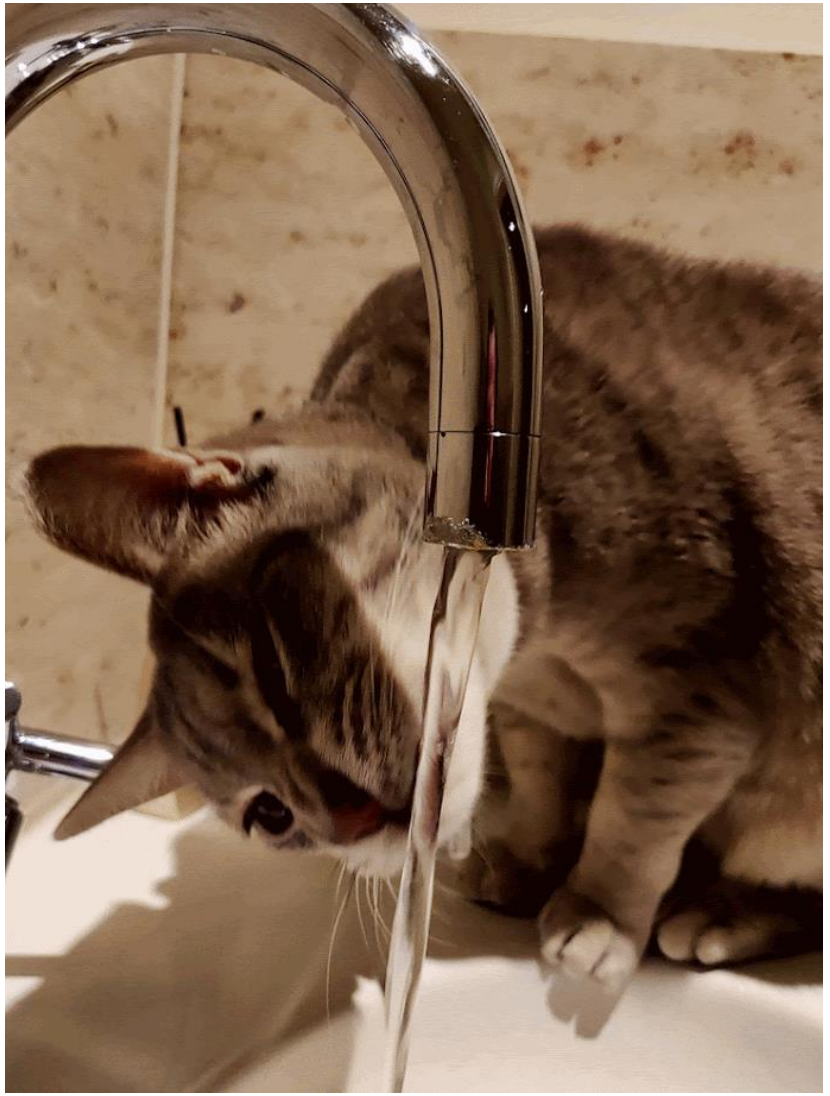
Lorem ipsum dolor set amet.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nam fermentum hendrerit lacinia. Cras feugiat, urna nec pharetra euismod, dui massa rhoncus dolor, ut commodo erat orci et

Severity	Unique	Total occurences
Critical	2	2
High	3	12
Medium	3	66
Low	1	1

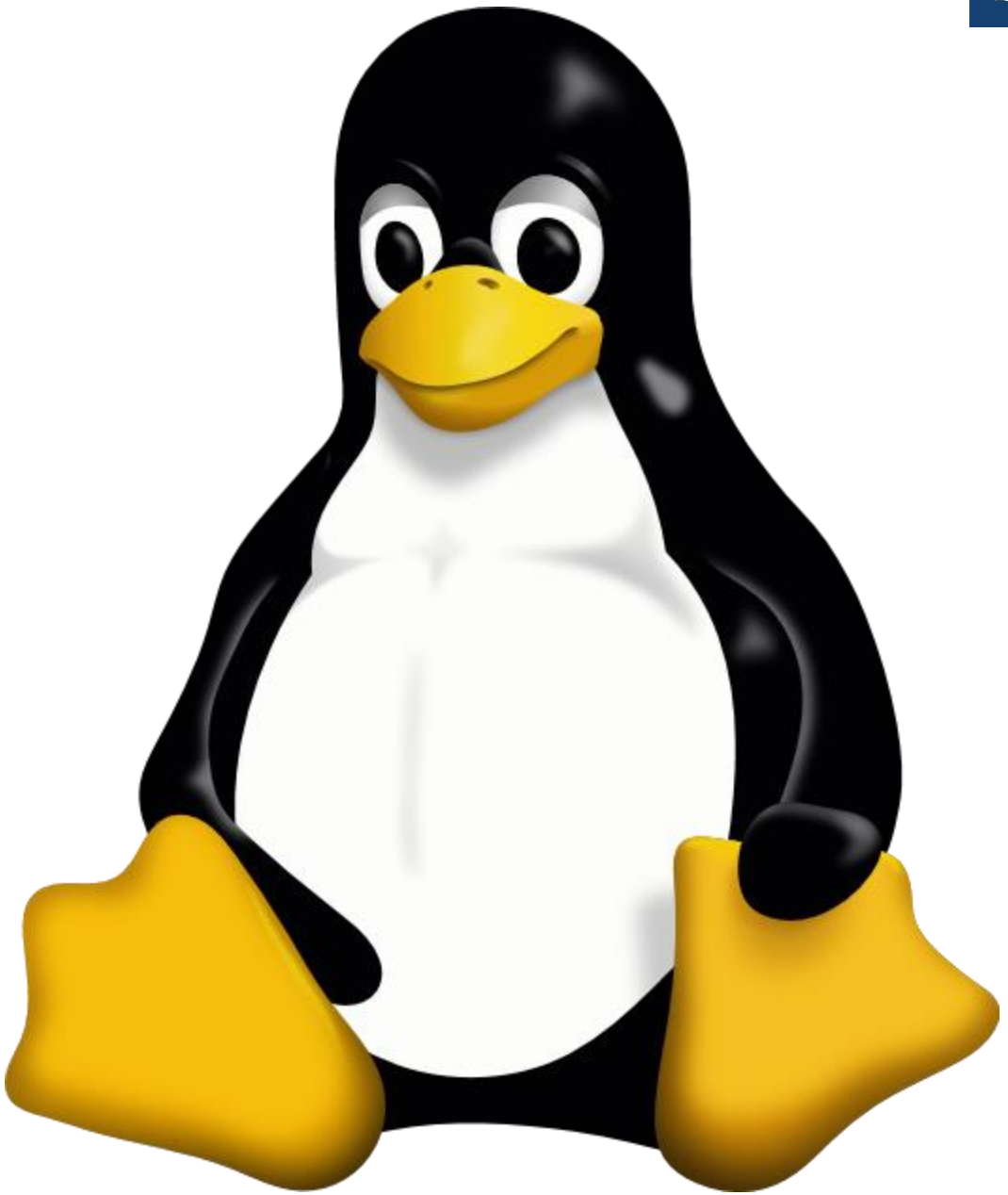
Realisatie 7: Doe alles forensisch accuraat

- Zorg dat we zoveel mogelijk bewijsbaar werken
- Boefjes in containerized omgeving met opslag input, output, netwerkverkeer, versieinformatie
- Records digitaal getekend en bewijsbaar dat iets op een bepaald moment in de tijd is gebeurd.
- Rapportages moeten forensisch accuraat zijn



Realisatie 8: Leer van Tux

- Werk zoals Linux:
  - Doe nooit zaken in grote problemen
  - Doe kleine taken
  - Bouw dat goed
  - Pak de verschillende zaken samen



10 Boefjes available

Show filter options

Nmap
Scans all 65000 ports behind an IP

See details Install & scan

Nmap250
Scans the 250 most popular ports behind an IP

See details Install & scan

SecurityHeaderDetection
Scans for missing HTML headers

See details Install & scan

CheckIfWebsite
Find websites behind a hostname

See details Install & scan

Nmap
Scans all 65000 ports behind an IP

See details Install & scan

Nmap250
Scans the 250 most popular ports behind an IP

See details Install & scan

SecurityHeaderDetection
Scans for missing HTML headers

See details Install & scan

DnsRecord
Collects all DNS records of a hostname

See details Install & scan

Realisatie 9: Niet zelf het wiel uitvinden

Gebruik bestaande software waar het kan

Realisatie 10: Beveiliging is een compliance-vraagstuk

Realisatie 11: Met de kennis van nu zouden we hier anders naar kijken

Je moet naar ieder moment in de tijd naar een object kunnen gaan

Objecten veranderen door de tijd heen door nieuwe regelgeving, ontdekte lekken, juridische constructen…

Veranderingen zijn het moment om business rules toe te passen

Findings over time

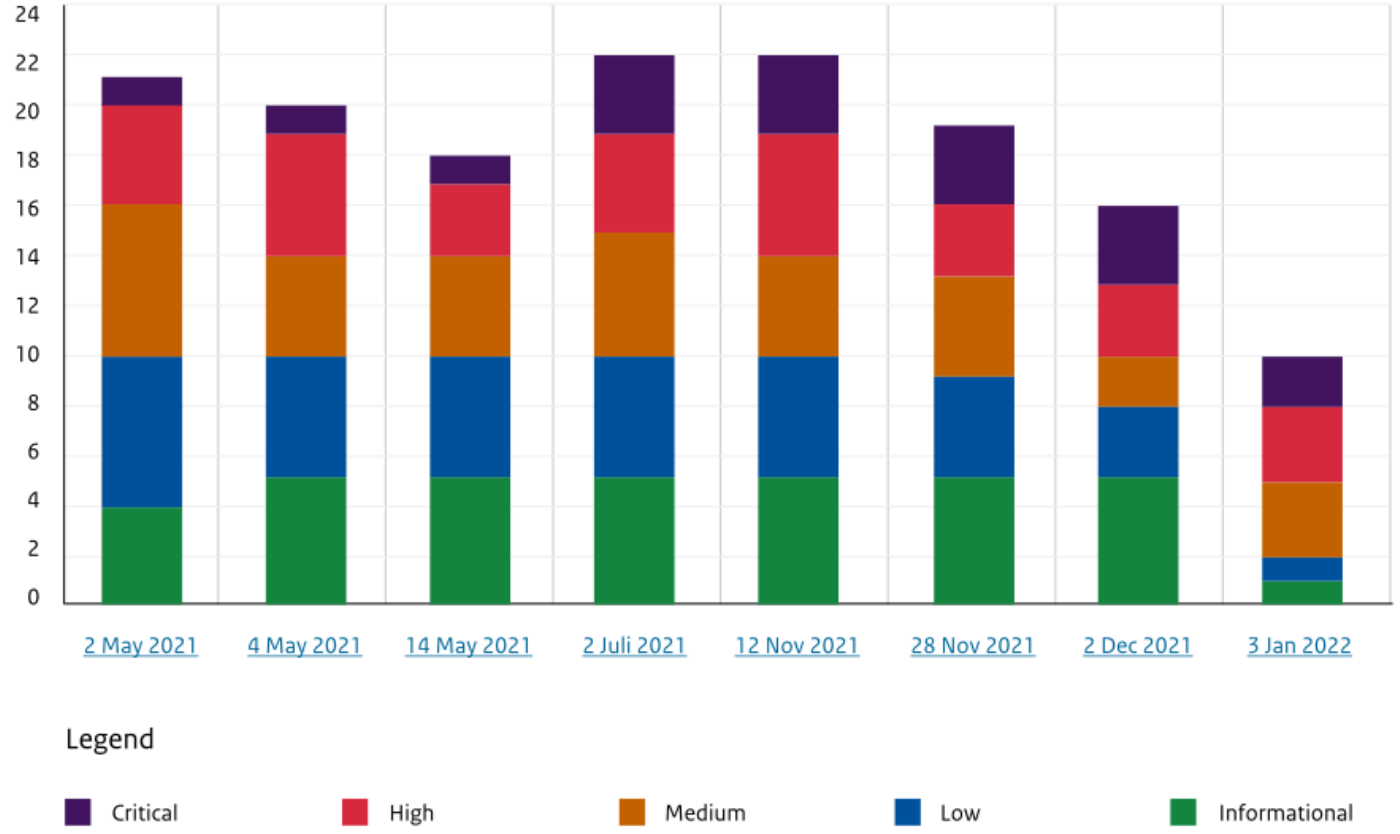
Comparing the current report to previous reports.

Over time issues can arrise or be solved. This graph gives a high overview of the current status compared to previous report(s). Giving insight into the number and type of issues.

Select one or mulitple reports to create a full and indepth comparison report.

Compare reports

Current report compared to previous reports.

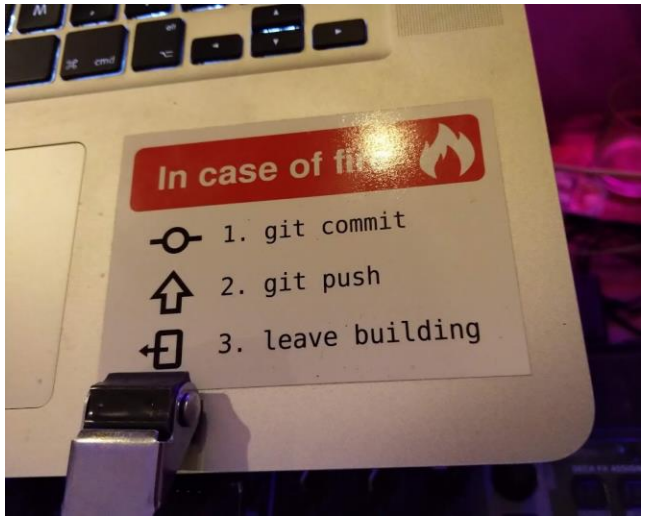


Findings

Number of findings compared between:

A: Pen Test Report example.org - Mrt. 4 2021 5:30pm - **B:** Pen Test Report example.org - Feb. 15 2021 4:31pm

Severity	Unique findings			Total occurrences		
	Most recent (A)	Previous (B)	Difference	Most recent (A)	Previous (B)	Difference
Critical	2	2	-1 +1 **0**	20	25	-8 +3 **-5**
High	3	3	- 0 + 0 **0**	12	16	-5 +1 **-4**
Medium	2	3	-2 +1 **-1**	20	25	-8 +3 **-5**
Low	3	6	-3 + 0 **-3**	12	16	-5 +1 **-4**
Informational	2	1	-1 +2 **+1**	20	25	-8 +3 **-5**



Kwetsbaarheden Analyse Tool

- KAT zoekt kwetsbaarheden in hele PDCA-cycle
- KAT bewaart een kopie van de werkelijkheid (foto)
- KAT 'snapt' de data die binnenkomt
- KAT automatiseert repetitief werk weg
- KAT borgt data bij binnenkomst forensisch
- KAT weet welk object bij welk proces hoort
- KAT levert bevindingen op basis van business rules:
  - Vulnerability scanning met logica van een pentester
  - SIEM-meldingen
  - Compliance
- KAT's bevindingen sluiten aan op het proces
- KAT gaat nog leveren:
  - Intelligente scheduling
  - Geautomatiseerde codereviews
  - Risico inschattingen (FMEA) op basis van processen

- Continuous pentesting
- Continuous monitoring
- Continuous compliance
- Continuous auditing
- Continuous risk assessment
- Continuous accountability

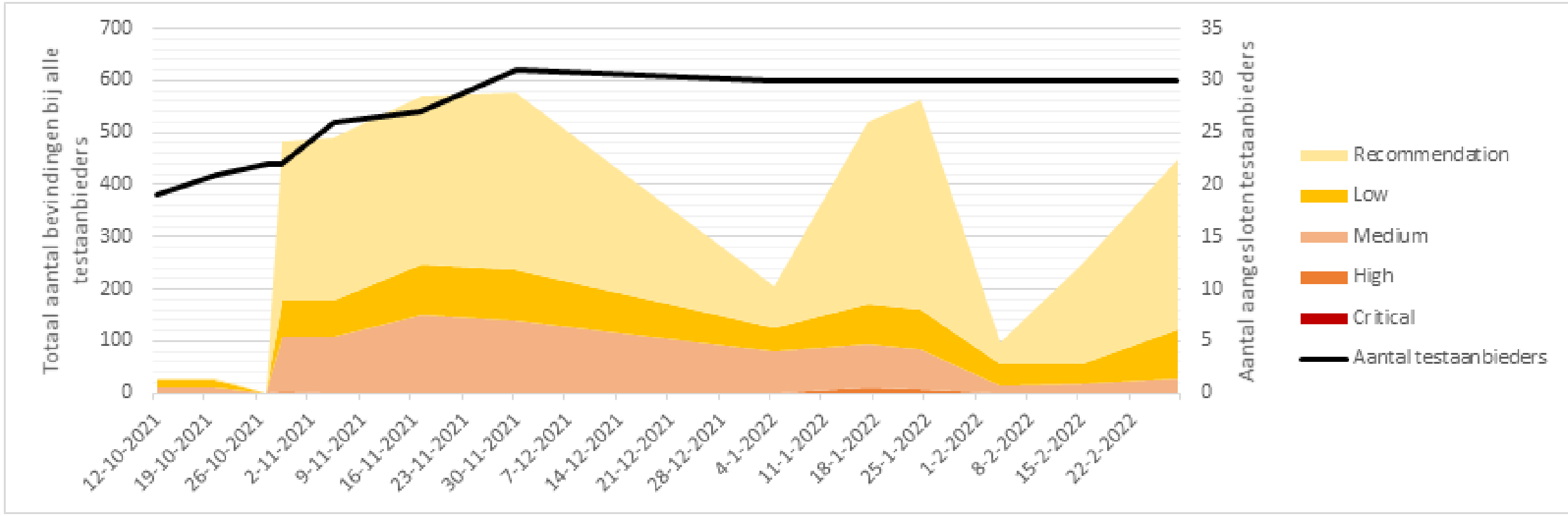
KAT is dus

Wat doen we dan?

Kwetsbaarheden Analyse Tool

4-10-2021

Testaanbieders



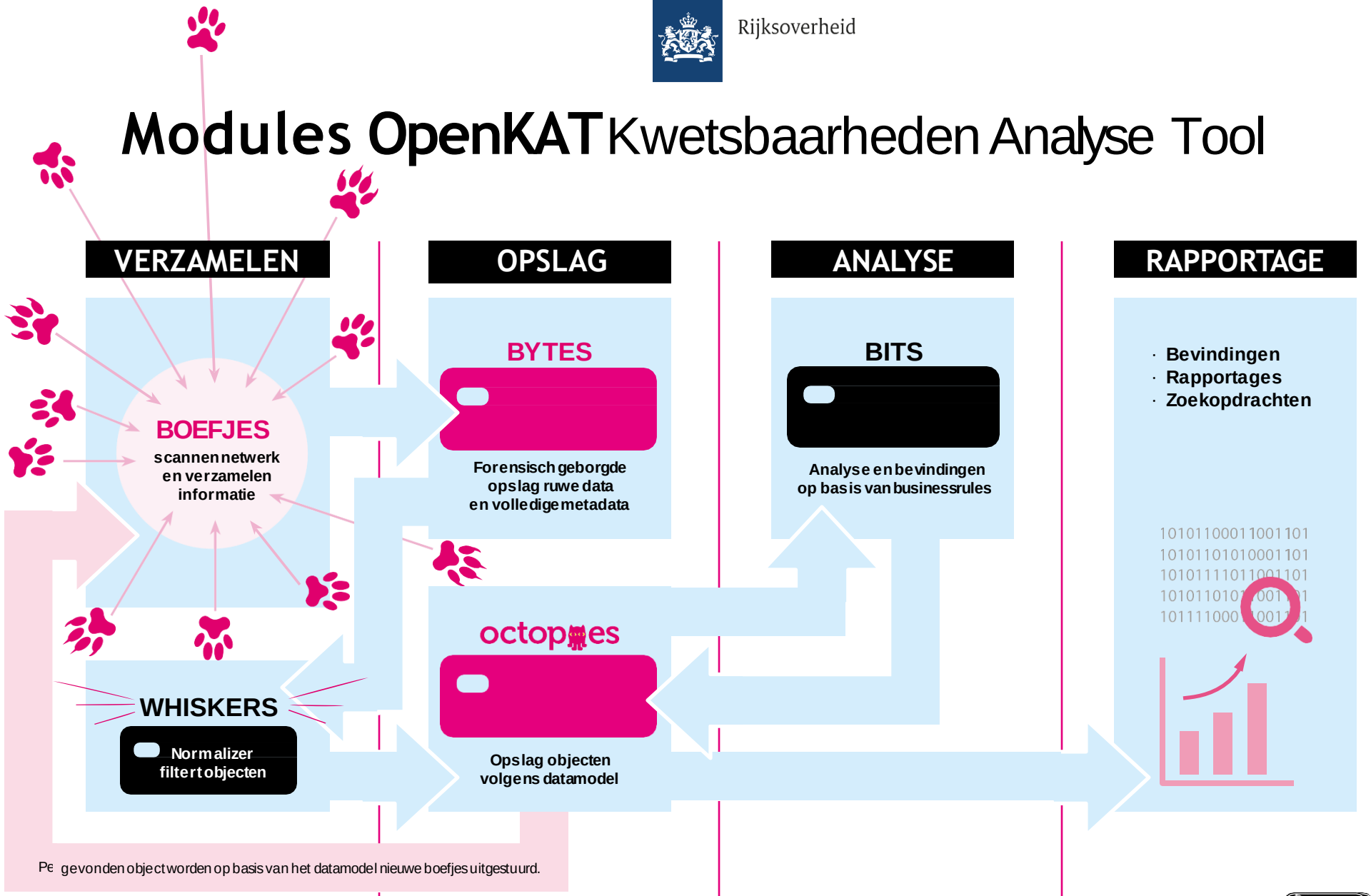
Ministerie van Volksgezondheid,
Welzijn en Sport

Een kijkje in de keuken van KAT

Overzicht van de onderdelen van KAT

Rijksoverheid

Modules OpenKAT Kwetsbaarheden Analyse Tool



Ministerie van Volksgezondheid,
Welzijn en Sport

Alle mogelijkheden in de: KAT-alogus

- Boefjes doen stukjes onderzoek
  - Vulnerability scan
  - API met informatie
  - Compliance checks
- Whiskers
- Decentraal
- Modulair onderdelen aan/uit zetten
- Kan achter firewall draaien
- Elke onderdeel genoemd naar een kat

KAT-acomben

octopoes

Forensisch geborgde kopie van de werkelijkheid

Temporal Graph-database – **exact weten, wanneer je wat hebt gezien**

Over meerdere setups overeenkomsten zien

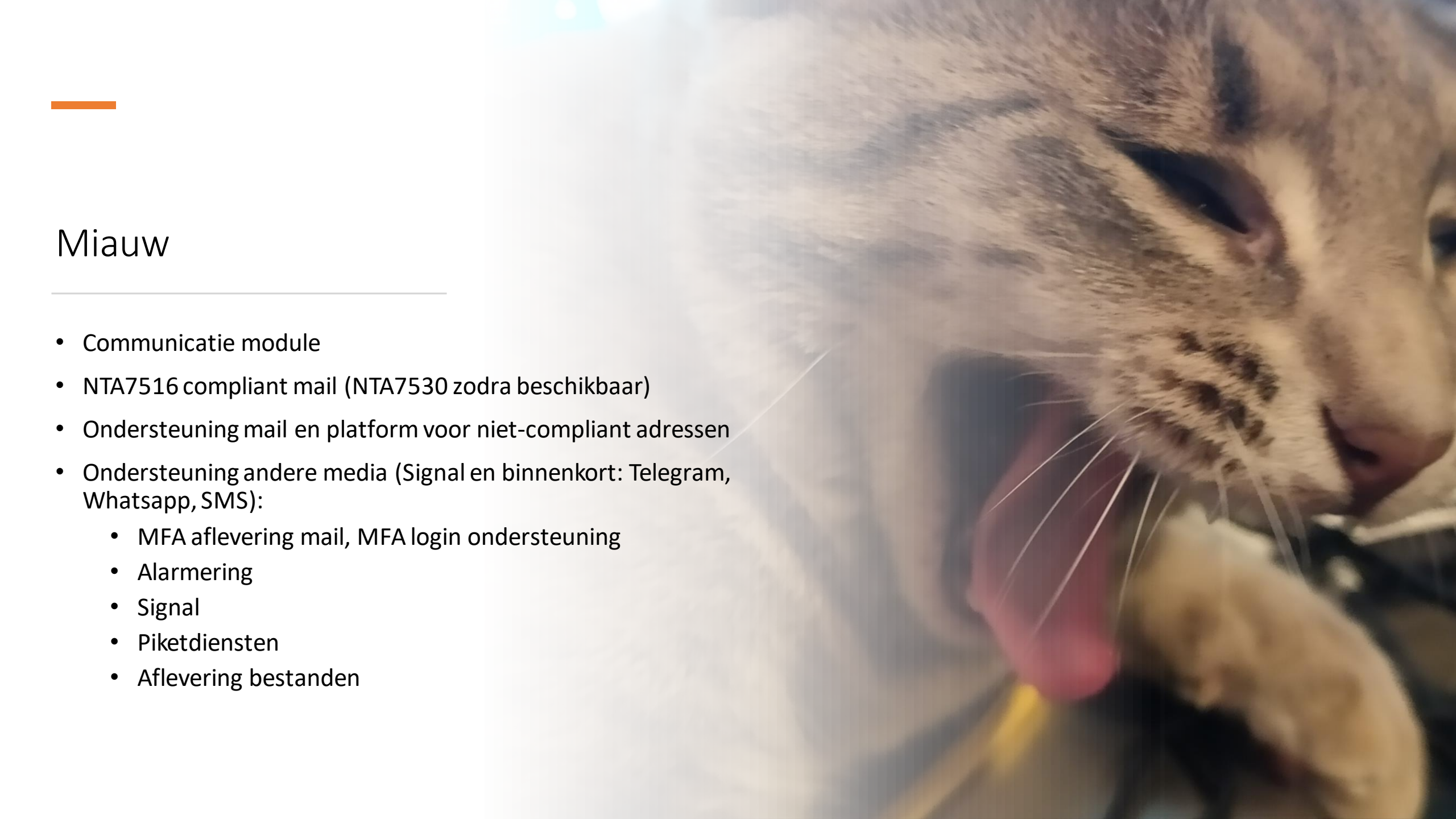
Veranderingen detecteren

Nieuwe inzichten (IOC's, queries) loslaten op oude data

Goede administratie van toestemmingen

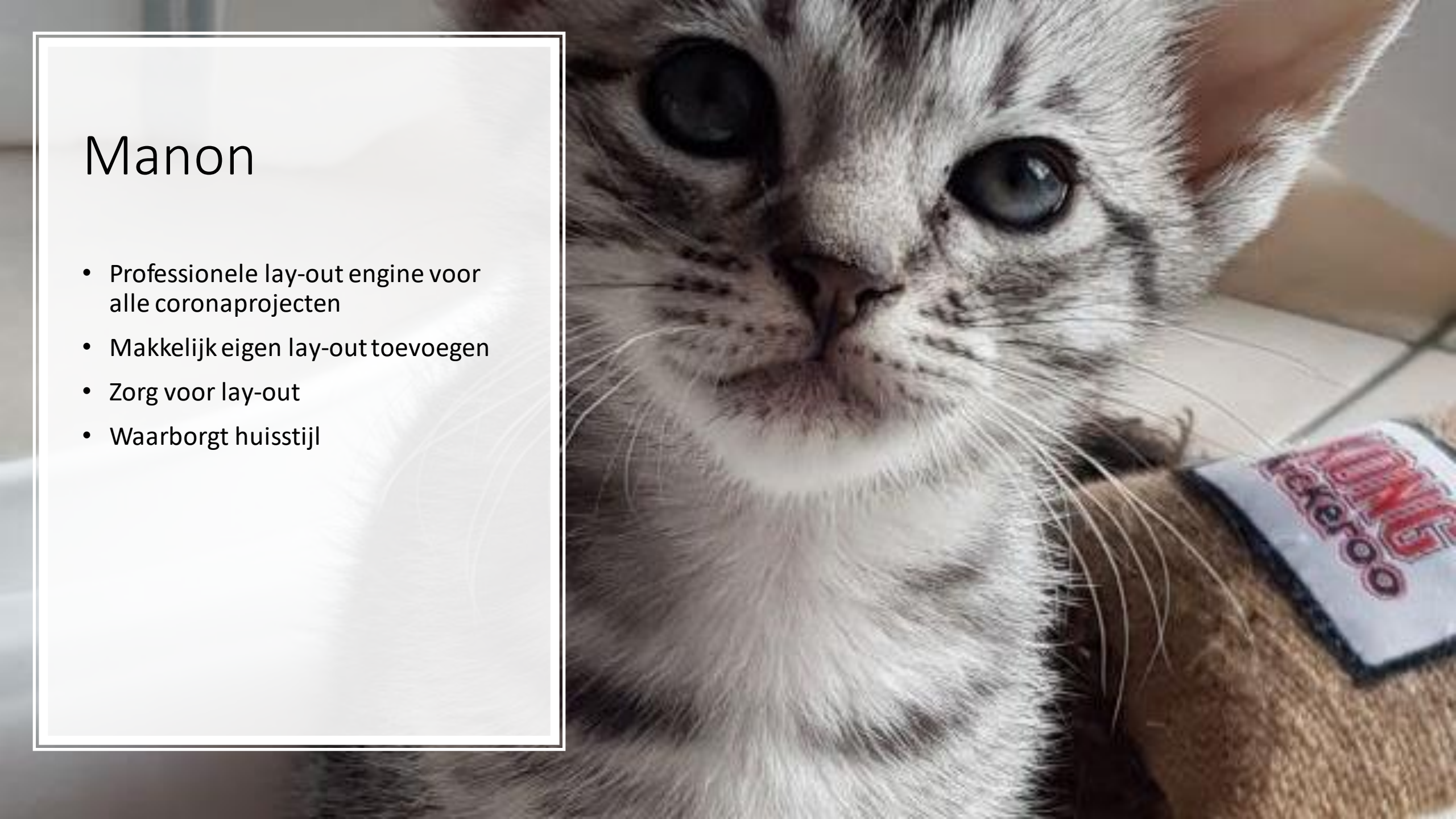
Miauw

- Communicatie module
- NTA7516 compliant mail (NTA7530 zodra beschikbaar)
- Ondersteuning mail en platform voor niet-compliant adressen
- Ondersteuning andere media (Signal en binnenkort: Telegram, Whatsapp, SMS):
  - MFA aflevering mail, MFA login ondersteuning
  - Alarmering
  - Signal
  - Piketdiensten
  - Aflevering bestanden



Manon

- Professionele lay-out engine voor alle coronaprojecten
- Makkelijk eigen lay-out toevoegen
- Zorg voor lay-out
- Waarborgt huisstijl



Rocky

- Interface voor alle interactie
  - Alle instellingen voor KAT
  - Hanteren gebruikersprofielen
  - Meertalig: Engels (binnenkort: Nederlands, Papiemento, Frysk)
  - Presentatie bevindingen
  - Graph
  - Doorzoeken vergaarde data (roadmap)
  - Invoeren van handmatige bevindingen
  - Invoeren/uitvoeren risicoinschattingen

Hiero

- Knowledgebase
- CVE, CWE, OWASP
- Waardevolle borging
- Geeft gebruikers context

Bits

- Bussiness rules engine
- Bepaalt of iets een bevinding wordt en met welke prioriteit
- Geeft context duiding binnen organisatie
- Helpt compliance te linken aan techniek
- Voorbeelden:
  - DigiD-pentest, WSTG-gebaseerde pentest
  - NTA-7516-compliance
  - Veranderingen in configuraties
  - Veranderingen in KVK
  - Voldoen aan toegankelijkheidsstandaarden
  - Cookie statement en correctheid ervan

Bytes

- Zorgt voor bewaren documenten
- Bewaart onderbouwing bij conclusies
- Waarborgt retentie termijnen
- Hashing voor audittrail
- Signing van hashes via externe provider voor forensische borging

Mula - Scheduler

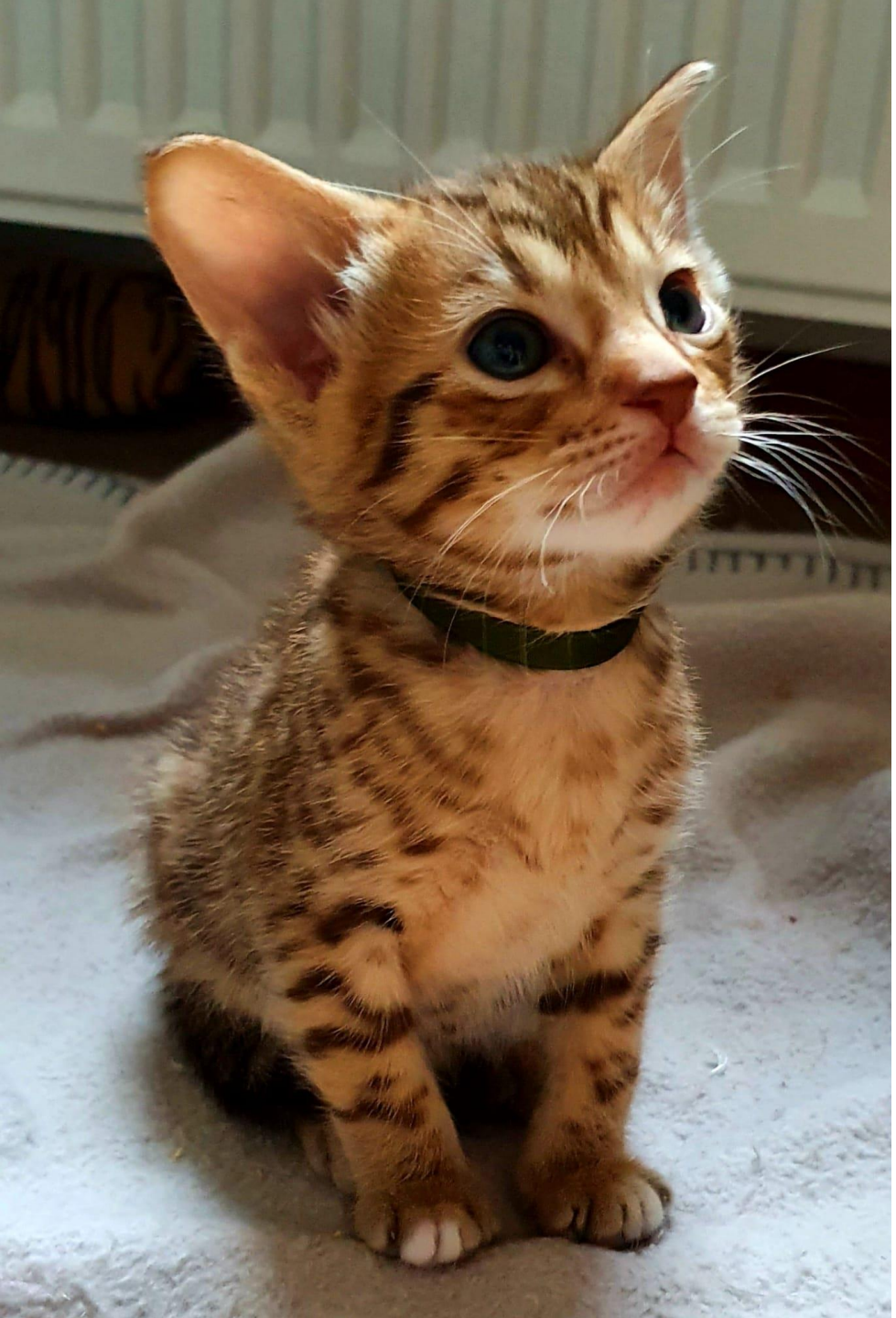
- Scheduling van offensieve acties
- Intelligent bepalen wat loont vaker te testen
- Goede administratie van vrijwaringen
- Hertesten bevindingen

Calvin

- Apache-Kafka filtering
- KSQL-use cases
- Statistische afwijkingen detecteren
- Doorzoeken logboeken op events
- Scannen van netwerk verkeer

Keiko

- Levert rapportages conform internationale standaarden bijvoorbeeld PTES
- Bundelt meerdere queries effectief
- Levert door forensische signing onafhankelijke, onweerlegbare rapportages



Otis (Roadmap)

- Inloggen via verschillende routes
  - Eigen stelsel
  - DigiD (eIDAS)
  - (iDIN?)
- Autorisatie management gebaseerd op rollen
  - Op basis van register
  - Functie binnen organisatie
- Forensisch geborgde digitale ondertekening

Artikel 15.
Deze algemene voorwaarden zijn in de Nederlandse en Engelse taal geste
van geschil over inhoud of strekking van deze algemene voorwaarden, za
Nederlandse tekst bindend zijn.

Verkoper
Getekend te Amsterdam op 30-11-2021 30-11-2021

DocuSigned by:
Brenno Johan Simon Aymard Alsgaard
292700FD47EC4D6...

DocuSigned by:
Charlotte Bidden
397FEACE8C73430...

Ministerie van Volksgezondheid,
Welzijn en Sport

Nu komt de kat op het koord...