



# Methodiek voor Informatiebeveiligingsonderzoek met Audit Waarde

Brenno de Winter



Wetgever **vereist**  
dat we kunnen  
bewijzen dat we  
in control zijn

- Algemene Verordening Gegevensbescherming (**AVG**)
- **NIS2, CRA**
- Hebben we zekerheden dat we zelf onderzoek hebben (**laten**) doen of leveranciers dat hebben gedaan?
- Normatieve kanten in kaders vervat (**ISO27001/NEN7510/BIO**)



# Aansprakelijkheden bij gebruik software

- **Artikel 82 AVG, eerste lid**
  - *Eenieder die materiële of immateriële schade heeft geleden ten gevolge van een inbreuk op deze verordening, heeft het recht om van de verwerkingsverantwoordelike of de verwerker schadevergoeding te ontvangen voor de geleden schade.*
- **Artikel 82 AVG, derde lid**
  - *Een verwerkingsverantwoordelijke of verwerker wordt van aansprakelijkheid op grond van lid 2 vrijgesteld indien hij bewijst dat hij op geen enkele wijze verantwoordelijk is voor het schadeveroorzakende feit.*

# De NIS2 eist meer helderheid

- NIS2 (artikel 32): De lidstaten zorgen ervoor dat de bevoegde autoriteiten bij de uitoefening van hun toezichthoudende taken met betrekking tot essentiële entiteiten de bevoegdheid hebben om deze entiteiten te onderwerpen aan ten minste:
  - (g) verzoeken om bewijs van de uitvoering van het cyberbeveiligingsbeleid, zoals de resultaten van beveiligingsaudits die door een gekwalificeerde auditor zijn uitgevoerd en de **respectieve onderliggende bewijzen**.
- NIS2 (artikel 33): De lidstaten zorgen ervoor dat de bevoegde autoriteiten bij de uitoefening van hun toezichthoudende taken met betrekking tot belangrijke entiteiten de bevoegdheid hebben om deze entiteiten te onderwerpen aan ten minste:
  - (f) verzoeken om bewijs van de uitvoering van het cyberbeveiligingsbeleid, zoals de resultaten van beveiligingsaudits die door een gekwalificeerde auditor zijn uitgevoerd en de **respectieve onderliggende bewijzen**.



De vraag is een  
pentest, die  
toont dat het  
**'goed zit'** ofwel  
bewijsvoering  
dat de  
bestuurder in  
control is.



# En de techniek?

Met de pentest van [BEDRIJF] weet je zeker dat je (web)applicatie, website, IT-infrastructuur, API's of mobiele apps kwetsbaarheden bevatten.

Natuurlijk wilt u hackers een stap voor blijven. Dit is waar een Pentest van pas komt, een beproefde methode om te testen of uw beveiliging van voldoende niveau is en werkt zoals verwacht. Wij vertellen u graag meer over dit effectieve middel om de IT-beveiliging te testen.

Met een penetratietest kunnen wij de ernst van IT-beveiligingsproblemen aantonen, zodat uw organisatie zich bewust wordt van de potentiële gevaren. Veel organisaties en bedrijven kiezen als direct gevolg van deze test voor een structurele aanpak van hun IT-beveiliging.

Laat u niet verrassen en laat regelmatig uw IT-infrastructuur controleren door de Hackers van Ons Bedrijf. Zo maakt u uw IT-infrastructuur weerbaar en bent u voorbereid op onbekende dreigingen.

**Het niveau en de staat van de digitale beveiliging kunnen bedrijven laten toetsen met een pentest.**

Met onze slimme, strategische en specifieke pentest test je meer dan alleen technologie. Veel meer. Je krijgt de exacte mikpunten in kaart voor cybercriminelen...

Door middel van een penetratietest (ook wel pentest genoemd) kan inzichtelijk worden gemaakt waar de risico's en kwetsbaarheden van de onderzochte systemen liggen.





# Dit bieden leveranciers

1. Ernst IT-beveiligingsproblemen aantonen
2. Infrastructuur weerbaar maken
3. Niveau en staat van de beveiliging aantonen
4. Risico's en kwetsbaarheden inzichtelijk maken
5. Testen of de beveiliging van voldoende niveau is
6. Mikpunten voor cybercrimelen in kaart brengen
7. Weten of je webapplicatie kwetsbaarheden bevat

# Hoe het vaak gaat: de magie van de Penetratietest

- Hoe we het doen is magie
- Wat we doen is bedrijfsgeheim
- Wat we opleveren mag je niet zomaar verspreiden
- En aan onze testen kun je geen rechten ontlenen



# Het **techno-optimisme** bij de klant: **Bij ons is alles veilig!**

---

- 'We hebben hackers laten kijken'
- 'We laten ons inspireren door de standaarden'
- Wat onze mensen doen is magie
- Wat een pentest is, tja dat is wat wij doen!
- Ze kwam er niet doorheen
- Zelfs hackers kregen het niet stuk

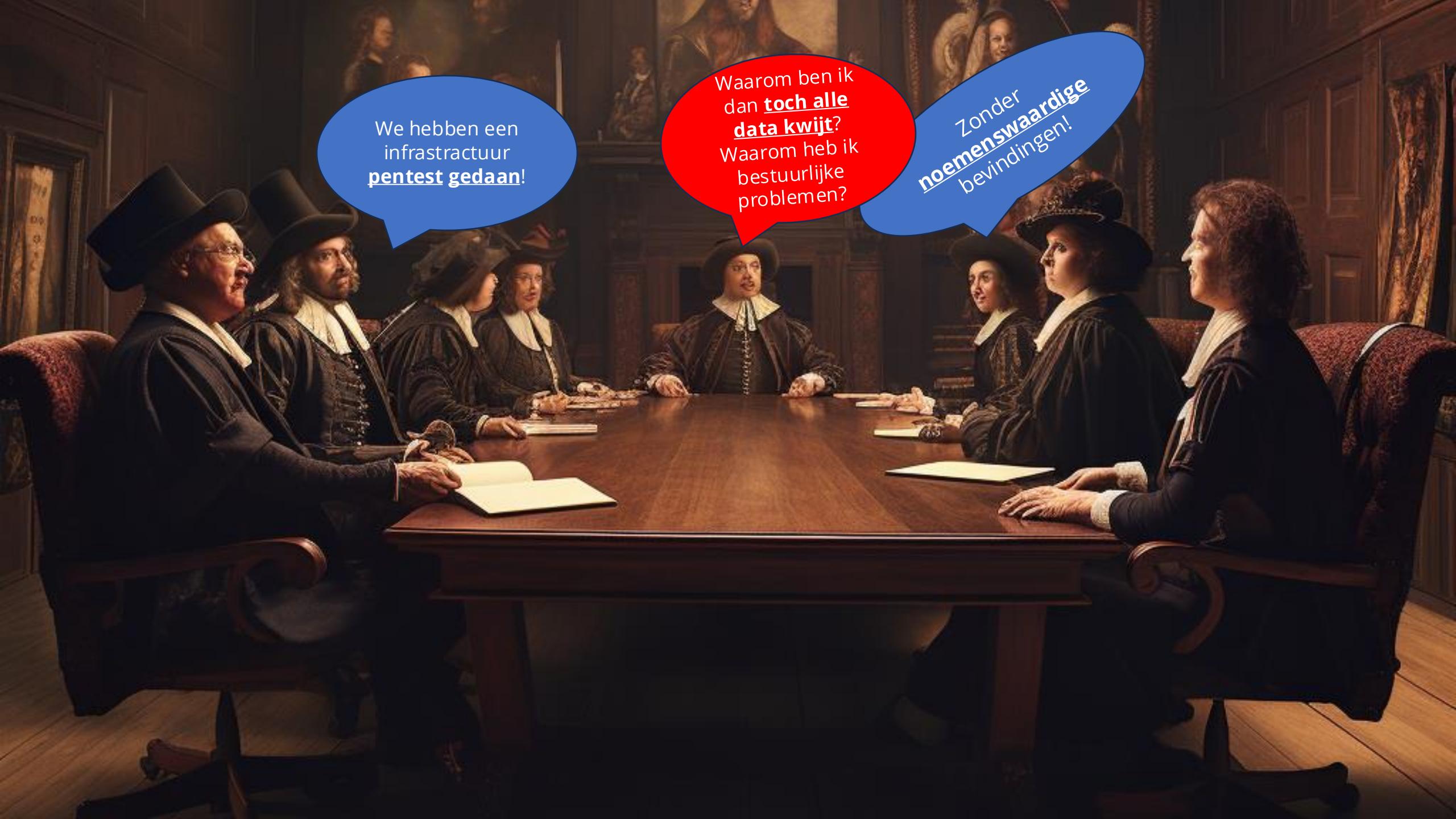




En vaak is **dit** de realiteit



Zes maanden later ...



We hebben een  
infrastructuur  
**pentest gedaan!**

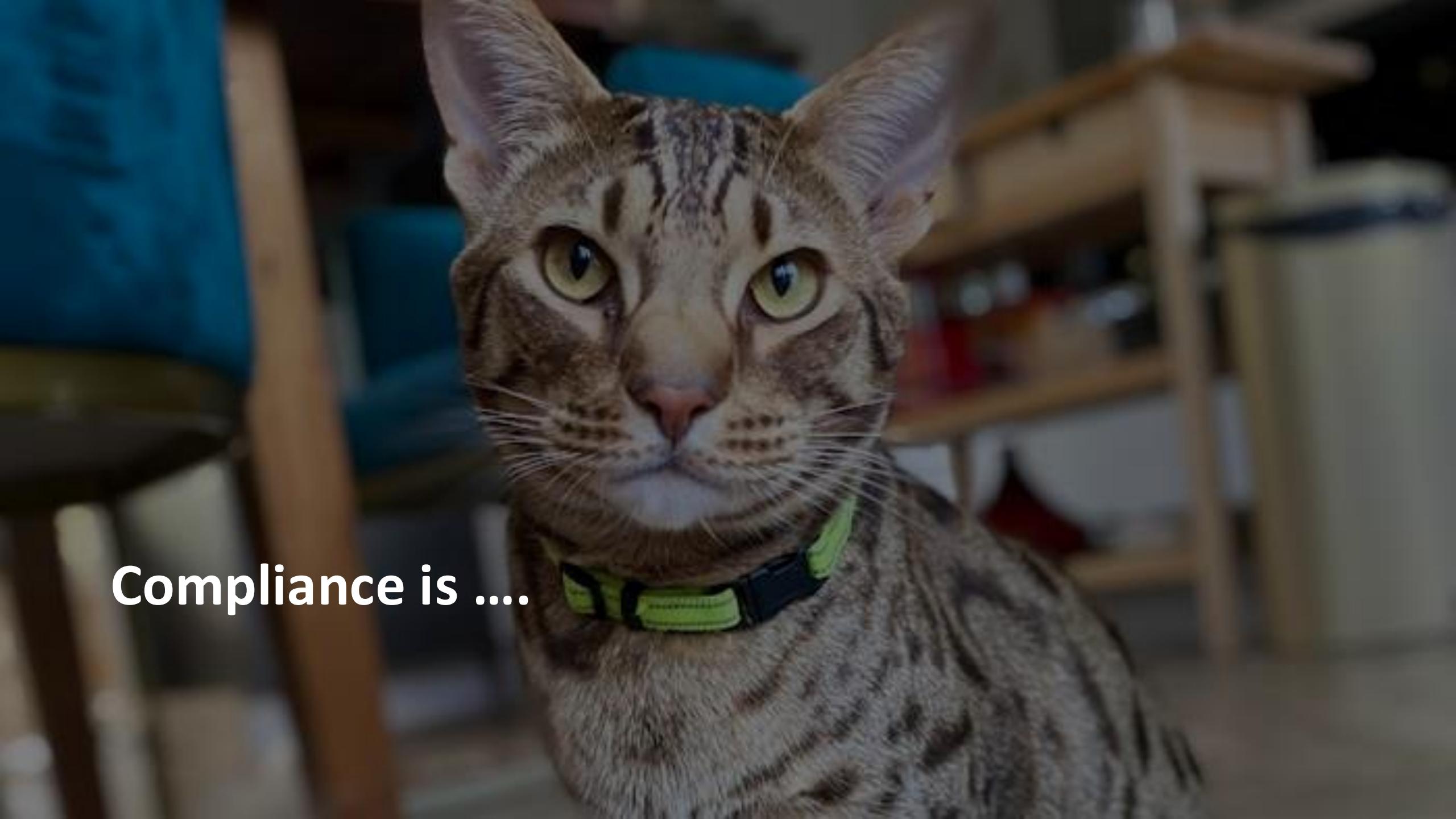
Waarom ben ik  
dan **toch alle**  
**data kwijt?**  
Waarom heb ik  
bestuurlijke  
problemen?

Zonder  
**noemenswaardige**  
bevindingen!

# Veel EU-regelgeving in tien jaar tijd (**tot 2026**)

- Artificial Intelligence Act (AIA)
- Artificial Liability Directive (AIL)
- Cyber Security Act (CSA)
- Data Act (DA)
- Digital Markets Act (DMA)
- Digital Operation Resilience Act (DORA)
- Digital Services Act (DSA)
- Directive on liability for defective products
- General Data Protection Regulation (GDPR)
- Network and Information Security Directive 2 (NIS2)
- Radio Equipment Directive
- Resilience of Critical Entities Directive (RCE)





Compliance is ....

# Bonus



Denk aan de  
jaarrekening

## SOC1 vs SOC2

### TRANSACTION & SECURITY PROCESSING CONTROLS FOCUS

Essential for revenue software

### SECURITY CONTROLS FOCUS

Essential for all service organizations  
including CLOUD service providers

Type 1 – opzet en  
bestaan

#### TYPE 1

- Organization system & controls
- At a specific time point
- Key security issues
- Opinion on design of controls

#### TYPE 2

- Organization system & controls
- Period of time
- Opinion on design & operating effectiveness of controls

#### TYPE 1

- Organization system & controls
- At a specific time point
- Focus on security

#### TYPE 2

- Organization system & controls
- Period of time
- Opinion on design & operating effectiveness of controls

Denk aan  
ISO 27001/2

Type 2 – werking



# Waar kijkt de auditor nou eigenlijk naar?

- 'We hebben hackers laten kijken' - geen vastgesteld kennisniveau
- 'We laten ons inspireren door de standaarden' - niet gestandaardiseerde tests
- Wat onze mensen doen is magie – **dark magic**
- Wat een **pentest** is, tja dat is wat wij doen! - geen kader



## De bredere vraag: Hoe voer je een audit uit?

- Is dat het toetsen van een claim?
- Is het terugkijkend?
- Is het vooruitkijkend?
- Is het overtuigd worden?

Waar stuur je op?



Tim Abang



# Uniform pentesten

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



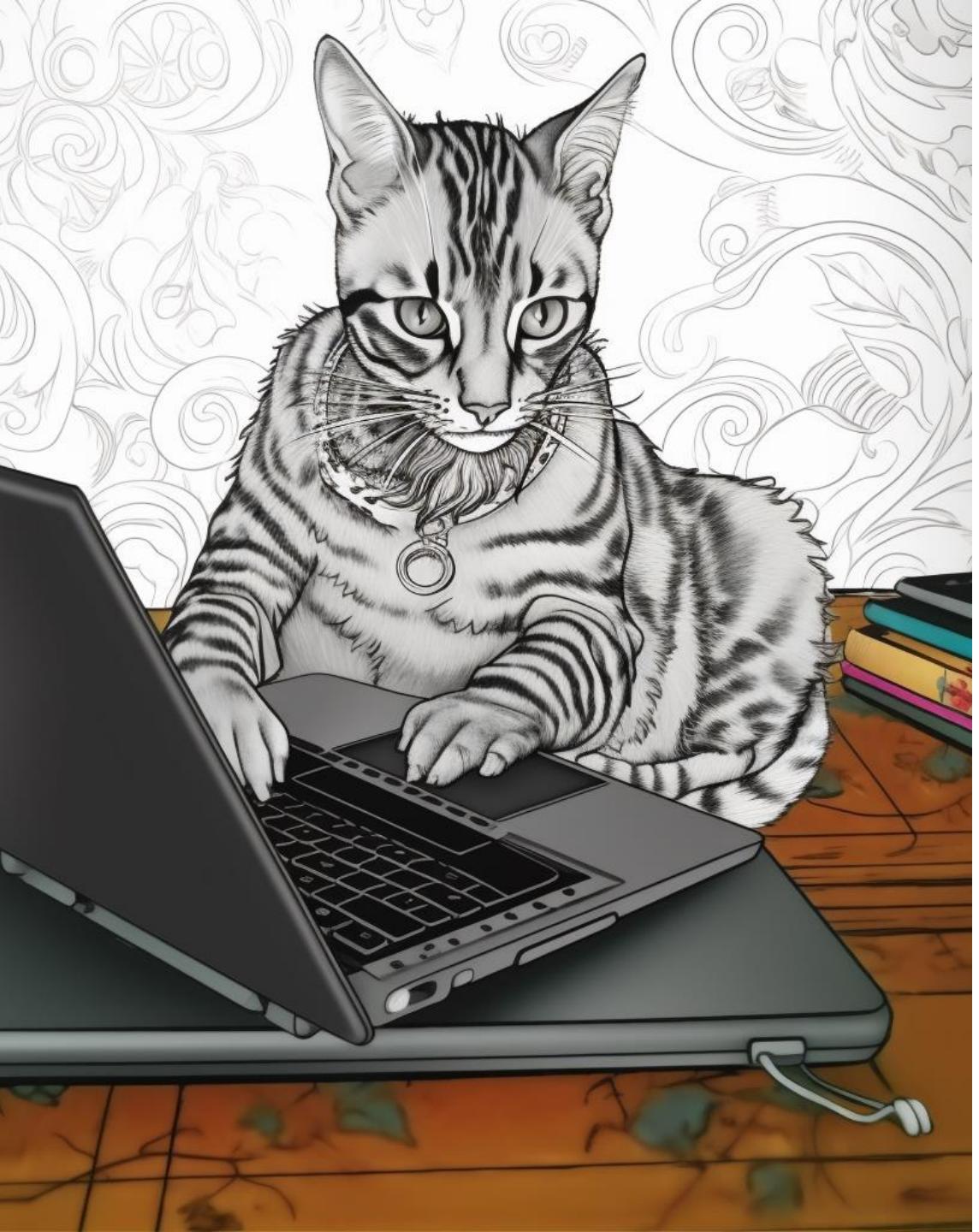
# **Repareerbaar** met wat chirurgische ingrepen

- Minder magie
- Meer zekerheid bieden
- Bewijs aanleveren



# Voor ieder type pentest





# Duidelijkheid definitie pentest

Penetratietest.

Een penetratietest (pentest) is "een door eigen personeel of derden uit te voeren offensief veiligheidsonderzoek, waarbij gecontroleerd wordt gezocht naar kwetsbaarheden in een of meer beveiligde netwerk- en informatiesystemen of onderdelen daarvan, die kunnen worden gebruikt voor het inbreken in deze systemen en/of die zonder opzet en autonoom de gegevensverwerking van de onderzochte organisatie kunnen verstören of anderszins nadelige gevolgen kunnen hebben".



# De 'hacker' ... nee ... onderzoeker heeft skills

De pentester kan dingen en heeft een relevante certificering

- OffSec Certified Professional (**OSCP**)
- OffSec Experienced Pentester (**OSEP**)
- OffSec Offensive Security Certified Expert (**OSCE** of **OSCE<sup>3</sup>**)
- OffSec Web Expert (**OSWE**)
- Web application Penetration Tester eXtreme (**eWPTX**)

# Een andere aanpak

- Pentest als container begrip met 'audit waarde'
- Bewijzen wat je hebt onderzocht en hoe
- Inkoopeisen
- Standaard hoe documentatie zou moeten werken



Opzet

Bestaan

Werking

# Onderzoeken volgens minimale set aan tests

- Uniforme eisen voor inkoop van pentesten
- Alle bevindingen langs dezelfde meetlat (CVSS) gewogen
- Duidelijke afspraken hoe je bevindingen opschrijft
- Een minimale set aan eisen:
  - OWASP MASTG/WSTG
  - CIS Benchmarks
- Uniforme manier van presenteren van bevindingen: PTES
- Reproduceerbaarheid van het onderzoek met inbegrip onderliggend bewijs
- De onderliggende tests worden meegeleverd
- Pentester zet handtekening
- Optioneel: Het rapport moet openbaar kunnen worden



# Beveiligingsonderzoeken

- Vulnerabilityscan
- Penetratietest
- Red Teaming
- Code review
- Security Assessment
- Zelf Conformiteitsbeoordeling
- Audit / Conformiteitsbeoordeling

A whimsical illustration of two fluffy kittens dressed as Superman, flying through a cloudy sky. The kitten on the left is slightly behind, looking towards the right. The kitten on the right is more prominent, looking directly forward with a determined expression. Both kittens are wearing blue superhero suits with red capes and yellow 'S' emblems on their chests.

# Na de pentest...

- Proces verbaal van bevindingen door 'een gekwalificeerd auditor'
- Betaalbaar geeft een summary op basis van het onderliggende document
- Geeft zekerheid over de onderliggende stukken

# **Methodiek voor informatiebeveiligingsonderzoek met Audit Waarde (MIAUW)**

Een open source pentest-standaard voor iedereen



Test ID	Description	Result
WSTG-INFO-01	Conduct search engine discovery and reconnaissance for information leakage	NOT PASSED
WSTG-INFO-02	Fingerprint web server	NOT PASSED
WSTG-INFO-03	Review web server meta files for information leakage	NOT PASSED
WSTG-INFO-04	Enumerate applications on web server	NOT PASSED
WSTG-INFO-05	Review webpage comments and meta data for information leakage	PASSED
WSTG-INFO-06	Identify application entry points	PASSED

		Y es	N o	Unknown
1.1.1	Disable unused filesystems			
1.1.1.1	Ensure mounting of cramfs filesystems is disabled			x
1.1.1.2	Ensure mounting of squashfs filesystems is disabled			x
1.1.1.3	Ensure mounting of udf filesystems is disabled			x
1.1.2	Configure /tmp			x
1.1.2.1	Ensure /tmp is a separate partition			x
1.1.2.2	Ensure nodev option is set on the /tmp partition			x
1.1.2.3	Ensure noexec option is set on the /tmp partition			x
1.1.2.4	Ensure nosuid option is set on the /tmp partition			x

# Wat is het?



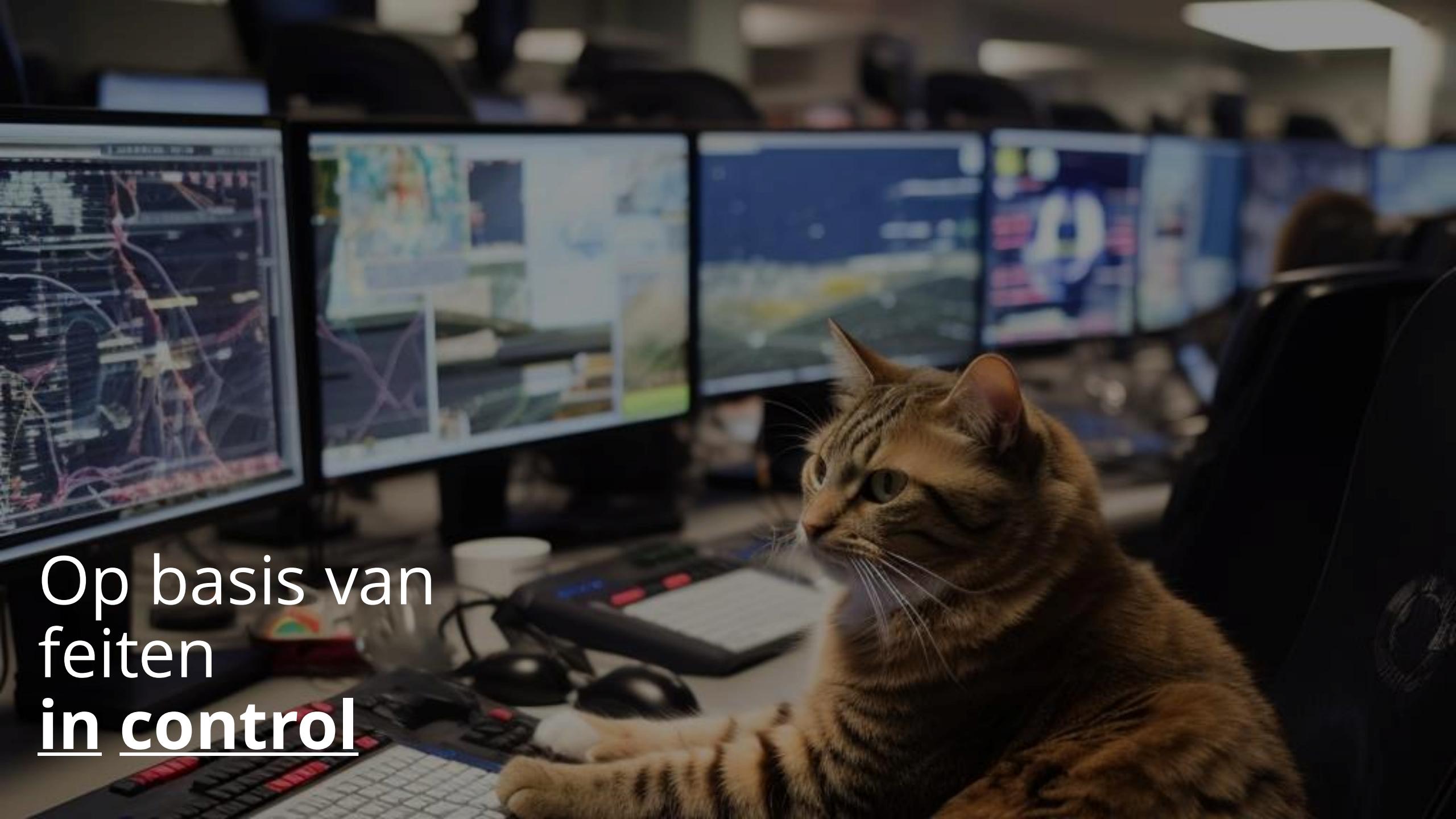
- Set aan controls voor een pentest:
  - Eis
  - Beschrijving
  - Hoe valideer je dit als auditor?
  - Wat krijg je hierdoor?
  - Wat mis je als je het niet hebt?
  - Hoe vraag je hierom in een aankoop?
- Model proces verbaal auditor
  - Correct doorlopen van het proces
  - Overzicht over de bevindingen
  - Bewijs dat voor de basics er wel of niet sprake is van in control zijn
- Model pentest rapportage
- Juridische informatie
- Een handleiding



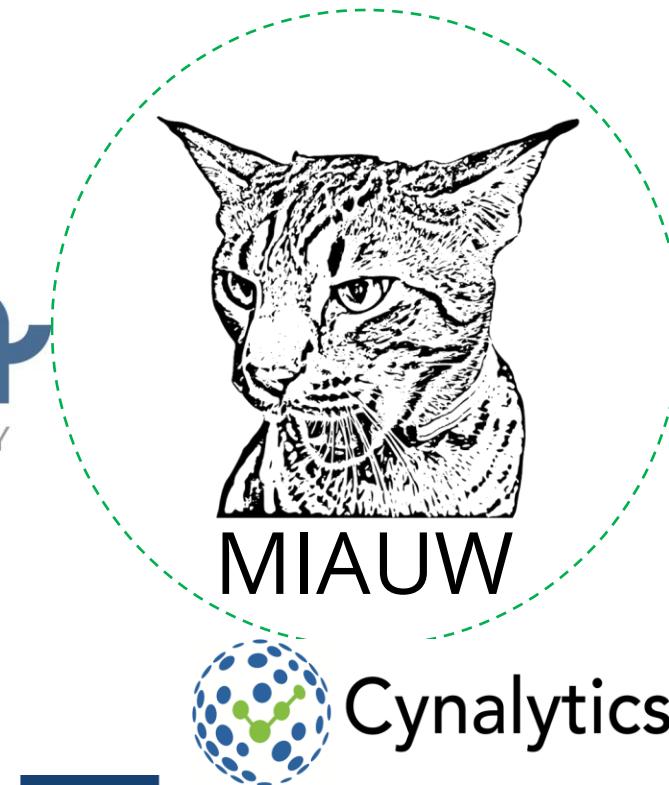
# Allemaal naar hetzelfde kijken



- Helderheid over wat er onderzocht is
- Helderheid over wat je niet hebt gekregen en wat dat betekent
- Helderheid of het onderzoek daadwerkelijk is uitgevoerd
- Reproduceerbaarheid
  - **Controleerbaar**
  - **Niet vaker dezelfde test doen**

A tiger-striped cat sits on a desk in a control room, looking towards the right. In the background, there are several computer monitors displaying various data and maps. A keyboard and a mouse are also visible on the desk.

Op basis van  
feiten  
**in control**



Ministerie van Volksgezondheid,  
Welzijn en Sport



Rijksdienst voor Identiteitsgegevens  
Ministerie van Binnenlandse Zaken en  
Koninkrijksrelaties