Making penentration testing auditable

Brenno de Winter

Legislator requires us to be able to prove we are in control

- General Data Protection Regulation (GDPR)
- **NIS2**, **CRA**
- Do we have assurances that we have (commissioned) our own research or suppliers have done so?
- Normative sides contained in frameworks (ISO27001/NEN7510/BIO)

Liabilities on use of software

- **Artikel 82 GDPR, first paragraph**
  - Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.
- **Artikel 82 GDPR, third paragraph**
  - A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.

NIS2 demands <u>more</u> clarity

- NIS2 (article 32): Member States shall ensure that the competent authorities, when exercising their supervisory tasks in relation to essential entities, have the power to subject those entities at least to:
  - (g) requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the **<u>respective underlying evidence</u>**.
- NIS2 (article 33): Member States shall ensure that the competent authorities, when exercising their supervisory tasks in relation to important entities, have the power to subject those entities at least to:
  - (f) requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the **<u>respective underlying evidence</u>**.

The question is: is a pentest, showing that things are ‘fine’ or proof that the director of the organization is in control.

En de techniek?

With [COMPANY]'s pen test, you can be sure that your (web) application, website, IT infrastructure, APIs or mobile apps contain vulnerabilities.

Naturally, you want to stay one step ahead of hackers. This is where a Pentest comes in handy, a proven method to test whether your security is of sufficient level and working as expected. We would be happy to tell you more about this effective means of testing IT security.

With a penetration test, we can demonstrate the severity of IT security problems, making your organisation aware of the potential dangers.

Many organisations and companies take a structural approach to their IT security as a direct result of this test.

Don't be taken by surprise and have your IT infrastructure regularly checked by Our Company's Hackers. This way, you will make your IT infrastructure resilient and be prepared for unknown threats.

Companies can have the level and state of digital security tested with a pen test.

With our smart, strategic and specific pentest, you test more than just technology. Much more. You get to map the exact target points for cybercriminals.

A penetration test (also known as a pentest) can reveal where the risks and vulnerabilities of the systems under investigation.

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 cybercriminelen in kaart brengen*
7. *Weten of je webapplicatie kwetsbaarheden bevat*

Hoe het vaak gaat: de **magie** van de Penetratietest

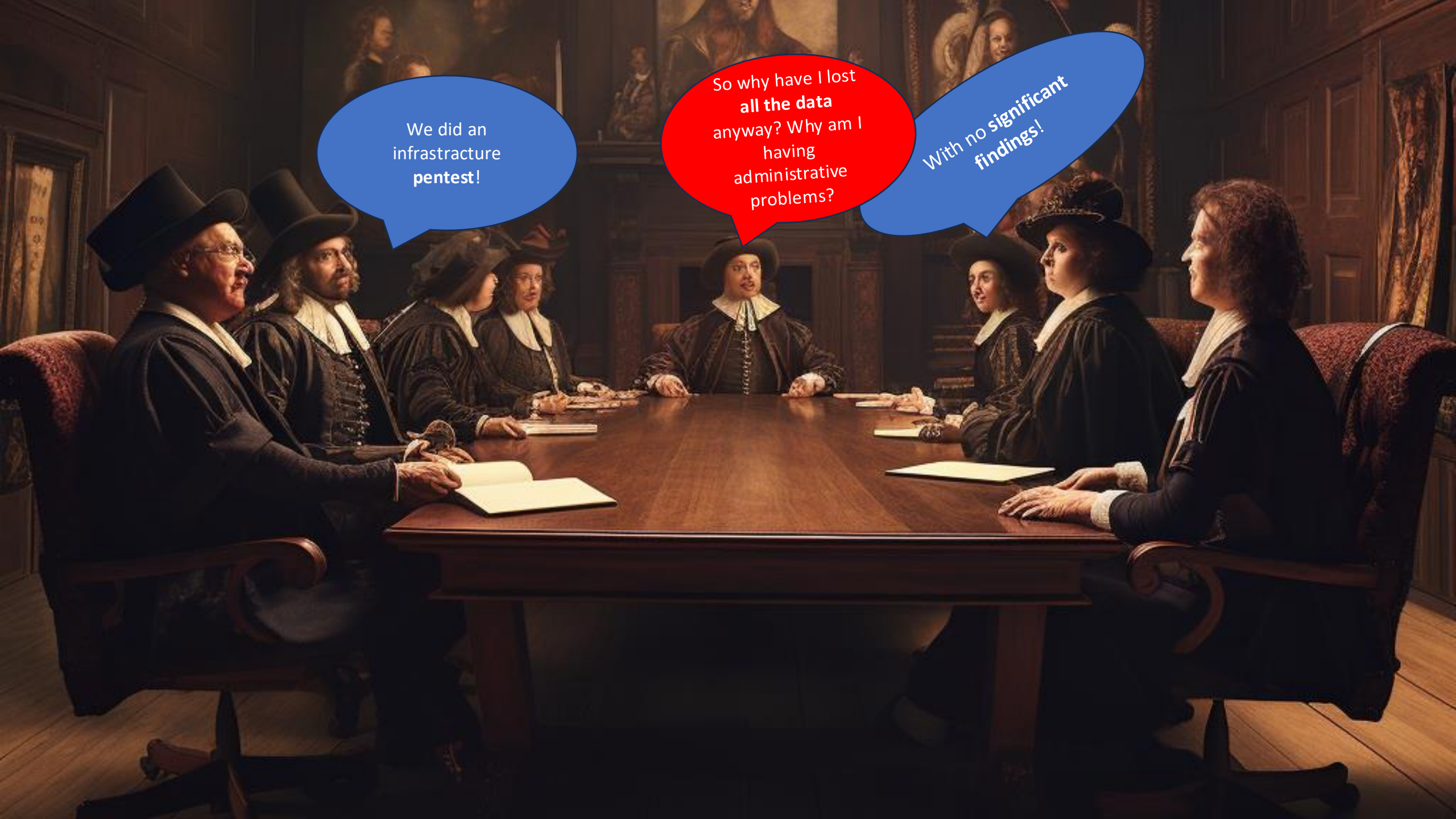
- Hoe we het doen is magie
- Wat we doen is bedrijfsgeheim
- Wat we opleveren mag je niet zomaar verspreiden
- En aan onze testen kun je geen rechten ontlenen

Customer techno-optimism: We are totally secure!

- ‘We've had hackers watching’
- ‘We take inspiration from standards’
- What our people do is magic
- What a pen test is, well that's what we do!
- She couldn't get through
- Even hackers couldn't get it broken

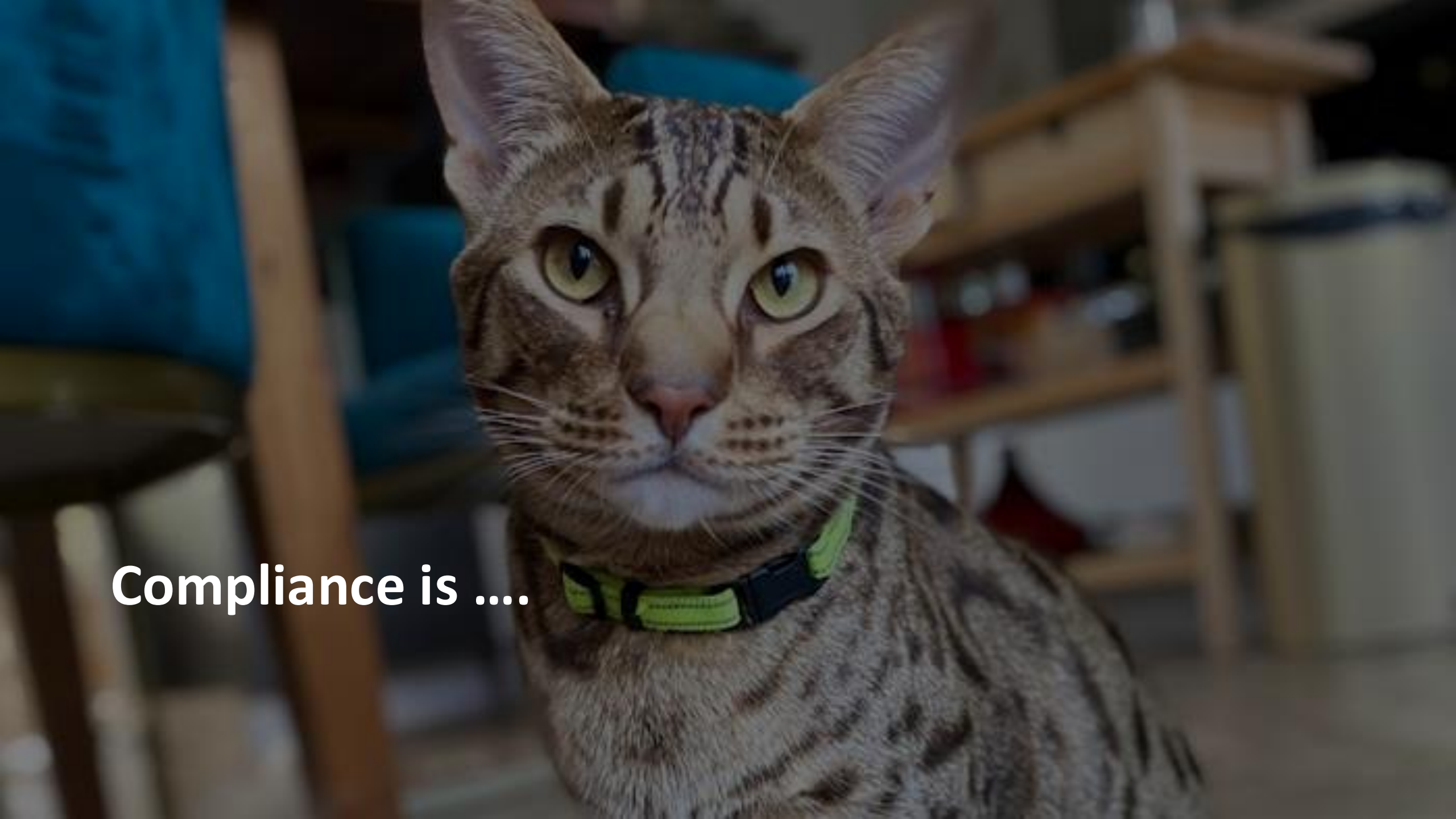
En vaak is **dit** de realiteit

Six months later ...


We did an infrastracture **pentest**!
So why have I lost **all the data** anyway? Why am I having administrative problems?
With no **significant findings**!

A lot of EU regulation in ten years (until 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

Financial statements

SOC1 vs SOC2

Think ISO 27001/2

TRANSACTION & SECURITY PROCESSING CONTROLS FOCUS		SECURITY CONTROLS FOCUS	
Essential for revenue software		Essential for all service organizations including CLOUD service providers	
TYPE 1	**TYPE 2**	**TYPE 1**	**TYPE 2**
• Organization system & controls • At a specific time point • Key security issues • Opinion on design of controls	• Organization system & controls • Period of time • Opinion on design & operating effectiveness of controls	• Organization system & controls • At a specific time point • Focus on security	• Organization system & controls • Period of time • Opinion on design & operating effectiveness of controls

Type 1 – **design** and **existence**

Type 2 – **operational effectiveness**

What is the **auditor** actually **looking at**?

- ‘We got hackers to look’ - no established level of knowledge
- ‘We take **inspiration from standards**’ - non-standardised tests
- What our people do is magic - **dark magic**
- What a **pen test** is, well that's what we do! - no framework

The broader question: How do you conduct an audit?

- Is that testing a claim?
- Is it looking back?
- Is it looking forward?
- Is it being convinced?

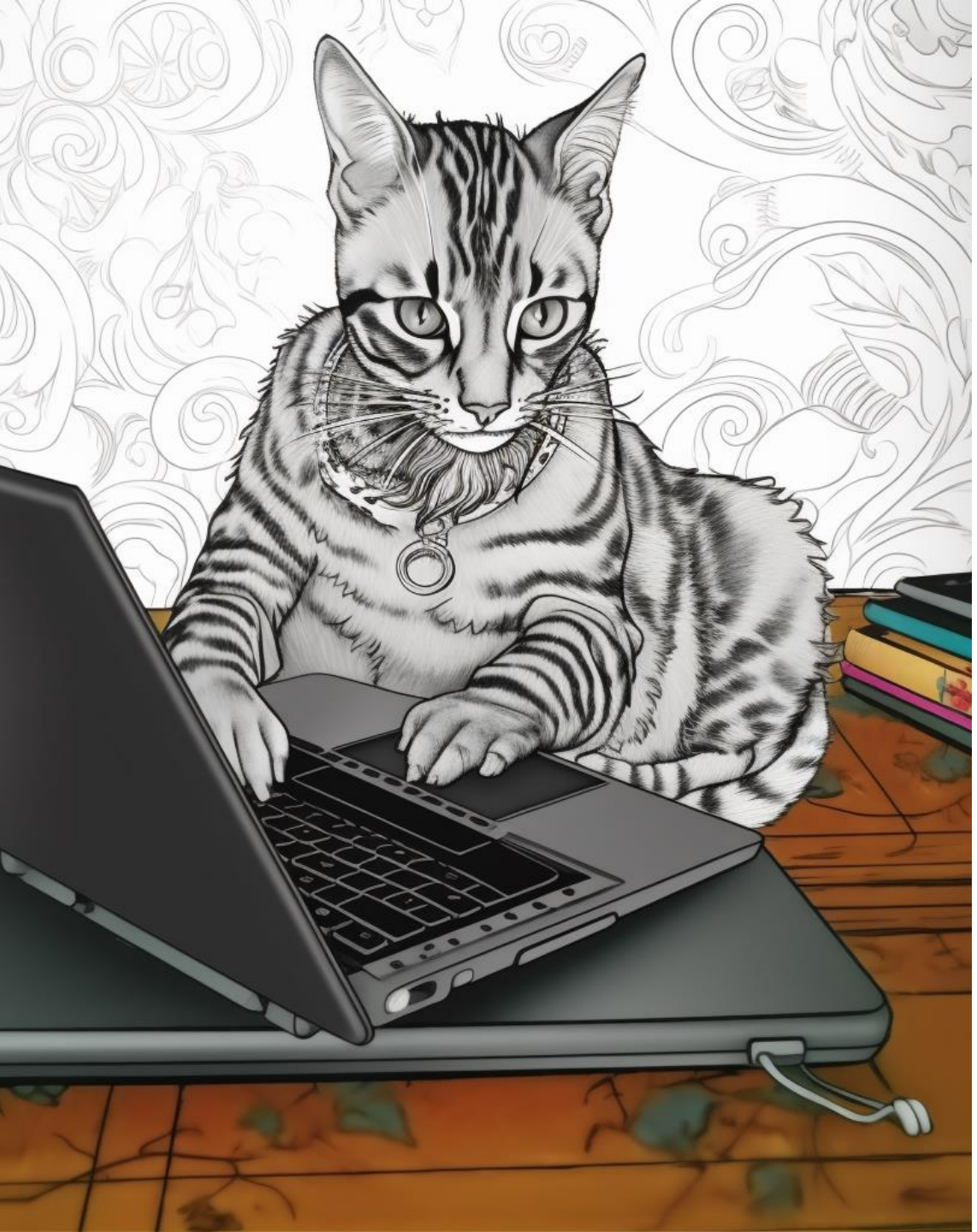
Wat do you steer towards?

Uniform **pen testing**

- Uniform requirements for procurement of pen tests
- All findings along the same yardstick (CVSS)
- A minimum set of requirements.
- OWASP **MASTG/WSTG**
- CIS **Benchmarks**
- Uniform way of presenting findings: **PTES**
- Reproducibility of the study
- The report will be publicly available

Repairable with some surgery

- Less magic
- Provide more certainty
- Providing evidence



Clarity definition **pentest**

Penetration test.

A penetration test (pen test) is '*an **offensive** **security** **investigation** to be carried outby its own personnel or third parties, which involves a **controlled** search for vulnerabilities in one or more secure network and information systems, or parts thereof, that could be used to **break into** these systems and/or that could **intentionally** **and** **autonomously** **disrupt** or otherwise **adversely** affect **the data processing** of the organisation under investigation'*.

The ‘hacker’ … no … researcher has **skills**

The pentester can do things and has relevant certification:

- OffSec Certified Professional (**OSCP**)
- OffSec Experienced Pentester (**OSEP**)
- OffSec Offensive Security Certified Expert (**OSCE** of **OSCE³**)
- OffSec Web Expert (**OSWE**)
- Web application Penetration Tester eXtreme (**eWPTX**)

A different approach

- Pentest as container concept with ‘audit value’
- Proving what you have investigated and how
- Procurement requirements
- Standard how documentation should work

Examination according to minimum set of tests

- Uniform requirements for procurement of pen tests
- All findings weighed against the same yardstick (CVSS)
- Clear agreements on how to write down findings
- A minimum set of requirements:
  - OWASP MASTG/WSTG
  - CIS Benchmarks
- Uniform way of presenting findings: PTES
- Reproducibility of the study including underlying evidence
- Underlying tests are included
- Pentester puts signature
- Optional: the report must be able to become public

Security surveys

- Vulnerability scan
- Penetration test
- Red Teaming
- Code review
- Security assessment
- Self Conformance Assessment
- Audit / Compliance assessment

After penetration testing …

- Report of findings by ‘a qualified auditor’
- Affordable provides a summary based on the underlying document
- Provides assurance on the underlying documents

Methodology for **information security research** with **Audit Value** (MIAUW)

An open source pentest standard for all

1.1.1	Disable unused filesystems	Yes	No	Unknown
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 seperate partition			X
1.1.2.2	Ensure nodev option is set on the /tmp partition			X
	Ensure noexec option is set on the /tmp partition			X

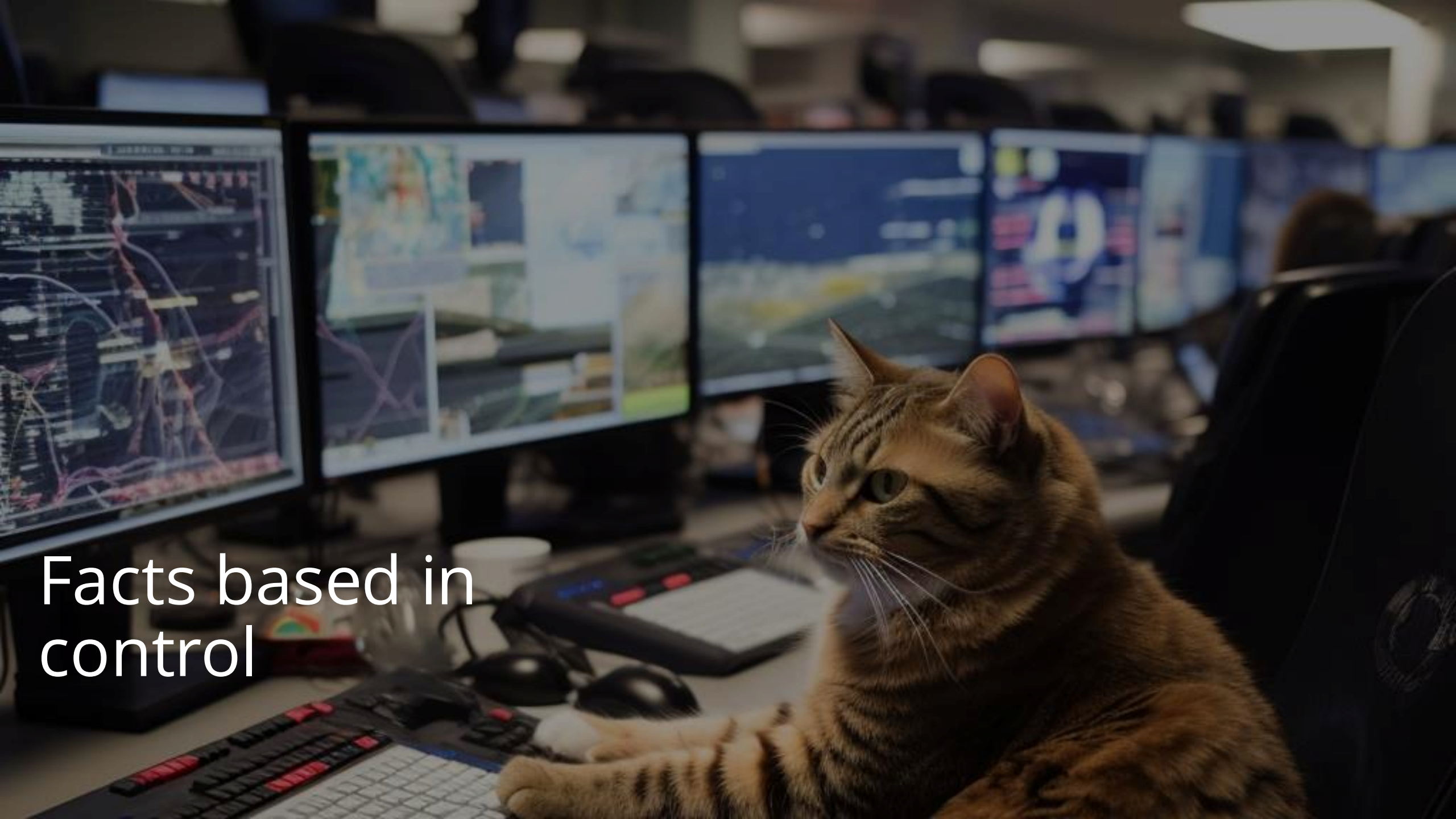
Test ID	Description	Result
WSTG-INFO-01	Conduct search engine discovery and reconnaissance for information leakage	NOT PASSED
WSTG-INFO-02	Fingerprint web server	NOT PASSED
WSTG-INFO-03	Review web server meta files for information leakage	NOT PASSED
WSTG-INFO-04	Enumerate applications on web server	NOT PASSED
WSTG-INFO-0505	Review webpage comments and meta data for information leakage	PASSED
WSTG-INFO-06	Identify application entry points	PASSED

What is it?

- Set of controls for a pen test:
  - Requirement
  - Description
  - How do you validate this as an auditor?
  - What do you get from this?
  - What are you missing if you don't have it?
  - How do you ask for this in procurement?
- Official procedural report by auditor:
  - Going through the process correctly
  - Overview of the findings
  - Evidence that for the basics there is or is not in control.
- A model pentest report
- Legal information
- An advisory guide on the ‘how to'

Looking at the same

- Clarity about what has been investigated
- Clarity about what you did not get and what that means
- Clarity about whether the research was actually carried out
- Reproducibility
  - **Verifiable**
  - **Not doing the same test more often**


Facts based in
control

ANOVUM
ONDERZOEK | STANDAARDEN | KENNISCENTRUM

ESET
Digital Security
Progress. Protected.

Mathison

De Winter Information Solutions

MR. V.A. DE POUS

OWASP®

UNICORN Security

DIVD

DSEC CONSULTING

NAGA CONSULTANCY

MIAUW

DIVD Academy

pinkroccade
TSS
LOCAL GOVERNMENT

Cynalytics

GROEN OPLOSSINGEN

OpenNovations

Ministerie van Volksgezondheid, Welzijn en Sport

Rijksdienst voor Identiteitsgegevens
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties