The Seven Sins.

And Virtues. Of IT Security. And how they affect our world.

What we can learn from ancient works,
ideas that actually matured quite well,
lessons from the past improving today.

A talk for BSides Munich 2023
The Reverend Father Heiderich.
mario@cure53.de

Our Dear Reverend

- **Reverend Father Mario Heiderich**
  - **Ex-Researcher and now Lecturer, Ruhr-Uni Bochum**
    - PhD Thesis about Client Side Security and Defense
    - Runs the course “Web & Browser-Security” at RUB
  - **Founder & Director of Cure53**
    - Pentest- & Security-Firm located in Berlin
    - Security, Consulting, Workshops, Trainings
  - **Published Author and Speaker**
    - Specialized on HTML5, DOM and SVG Security
    - JavaScript, XSS and Client Side Attacks
  - **Maintains DOMPurify**
    - A top notch JS-only Sanitizer, also, couple of other projects
  - **Can be reached out to as follows**
    - mario@cure53.de
    - +49 1520 8675782

Disclaimer

**I come in peace, mean no offense and,
if offense is taken nevertheless,
apologies and please let me know
so I can do better next time.**

Keynote Structure

Sermon One: Seven Sins
What people do despite knowing not to.

Sermon Two: Seven Virtues
What people should do, but usually won’t.

Sermon Three: Pathway to Heaven
How to get there no matter the hardship.

First Sermon

The Seven Sins

The Seven Sins: Origins

- **Ancient Origins build a foundation**
  - Roman writers, e.g. **Horace** extolled virtues
  - They also listed and warned against vices
  - Getting rid of folly is the beginning of wisdom
- **Christian concepts slowly manifest**
  - Early 4th Century, written in a monastery
  - **Evagrius Ponticus**, one of those who documented
  - He created a list of *eight* evil thoughts & temptations

“Your village
is under attack!”

The Seven Sins: Origins

- **Gula** (gluttony)
- **Luxuria/Fornicatio** (lust, fornication)
- **Avaritia** (avarice/greed)
- **Tristitia** (sorrow/despair/despondency)
- **Ira** (wrath)
- **Acedia** (sloth)
- **Vanagloria** (vainglory)
- **Superbia** (pride, hubris)

The Seven Sins: Refined

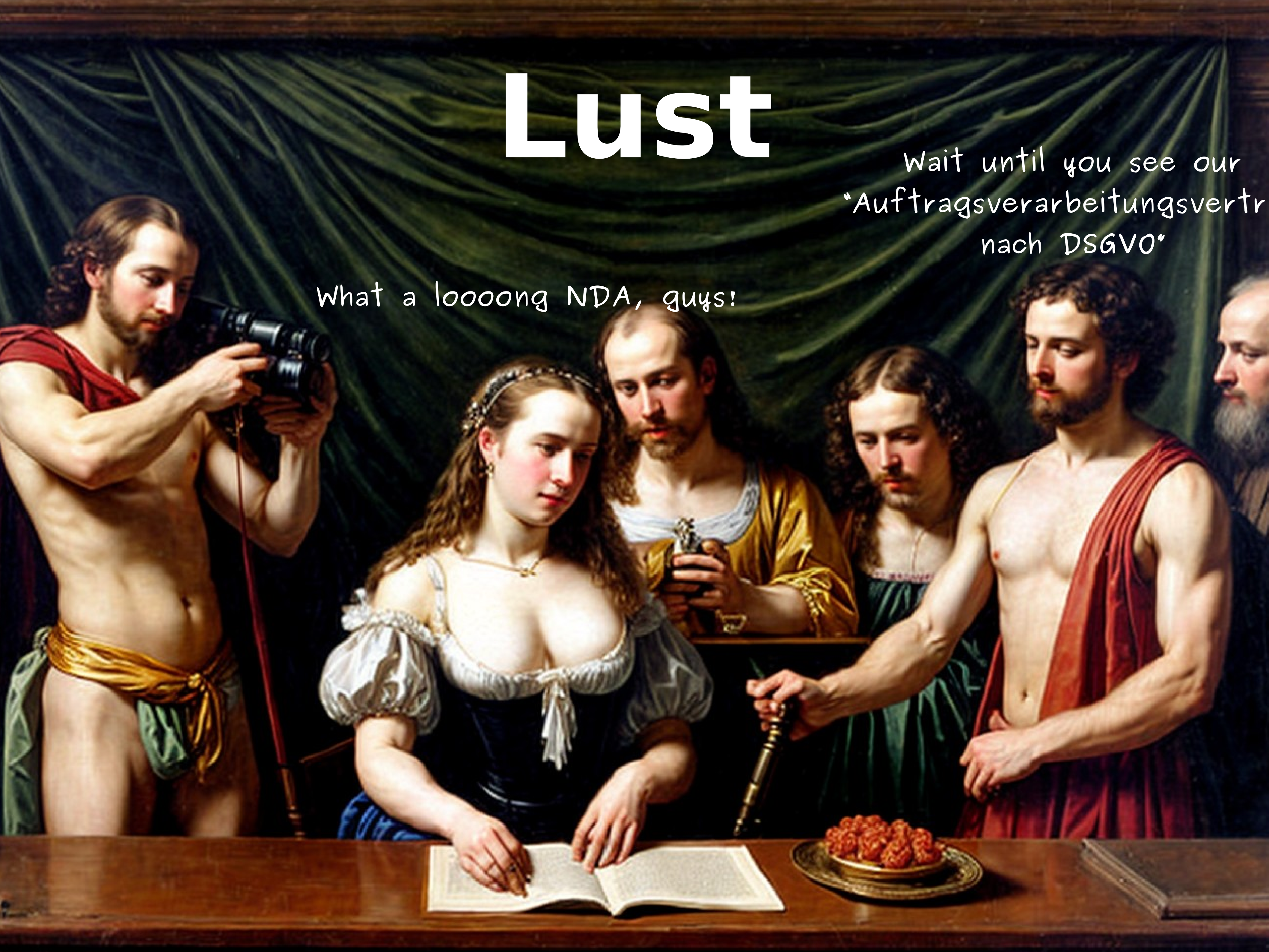
- **They are "deadly" because they lead to *spiritual* death**
- **In the 6th century, Pope Gregory the 1st revised this list**
- **This came out as the final release candidate**
  - Lust
  - Gluttony
  - Greed
  - Sloth
  - Wrath
  - Envy
  - Pride
- **Dante's "Divine Comedy" helped them become a hit**
- **Pretty much just like the OWASP Top Ten**

Lust

Lust

And action!

Lust


Wait until you see our “Auftragsverarbeitungsvertr nach DSGVO“
What a loooong NDA, guys!

Lust – or uncontrolled Desire

- **This often manifests as desire to access, control, data, and well - power**
  - Or to exploit systems and data without having proper authorization or need.
  - Or to gather too much data from fellow users.
- **Or an overzealous adoption of new technologies without proper risk assessment or security review**
  - Just put an AI on MDN and see what will happen, LOL.
  - This problem can only be solved by blockchain and NFTs
- **Or simply engaging in overlong discussions on a bug bounty platform**

Gluttony

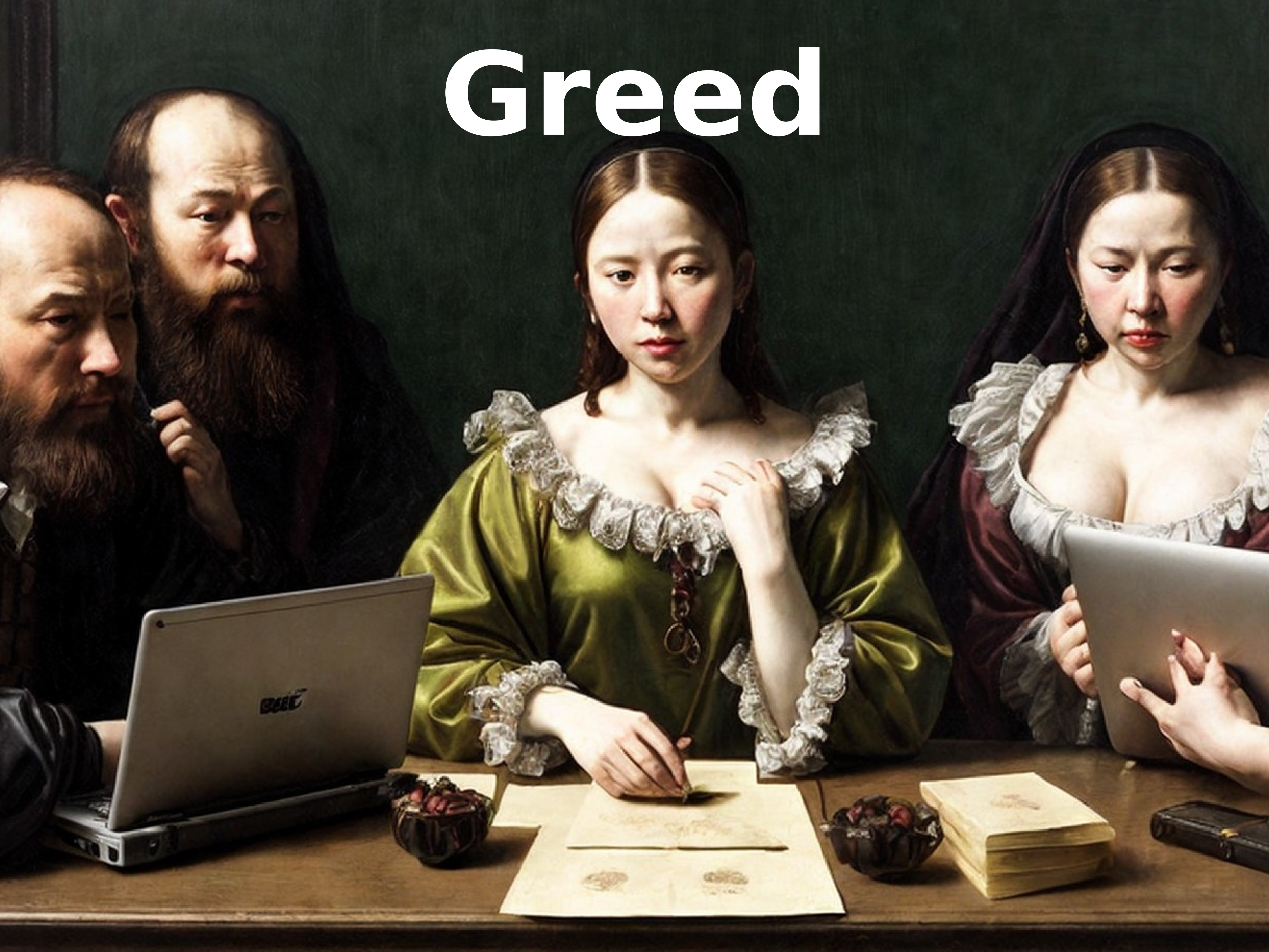
Gluttony

Gluttony

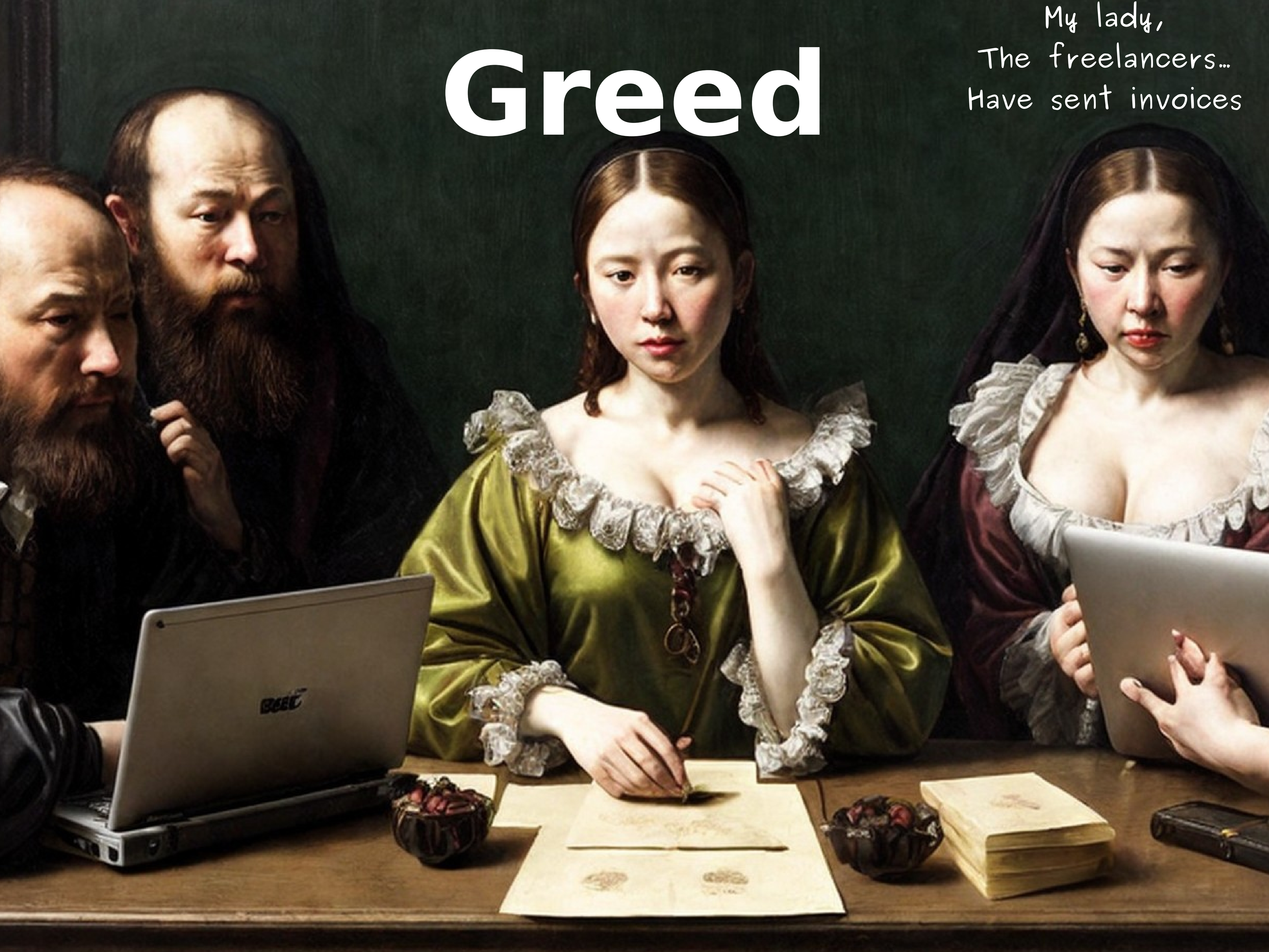
Gluttony – or Overindulgence

- **This can easily be equated with hoarding data.**
  - Organizations often collect and store more data than they need, increasing their risk exposure if there's a data breach.
  - In Germany we say “Datenreichtum” which is lovely
- **Over-consumption of resources can lead to inefficiencies or vulnerabilities.**
  - This holds for technology of course
  - But most importantly for humans too! Stressed developers cannot write bug-free code.
- **Or simply not spending money where it’s needed**
  - Security Training for development or a new Mercedes for the CEO?
  - You can’t go 280 km/h with a well -trained developer can you?

Greed

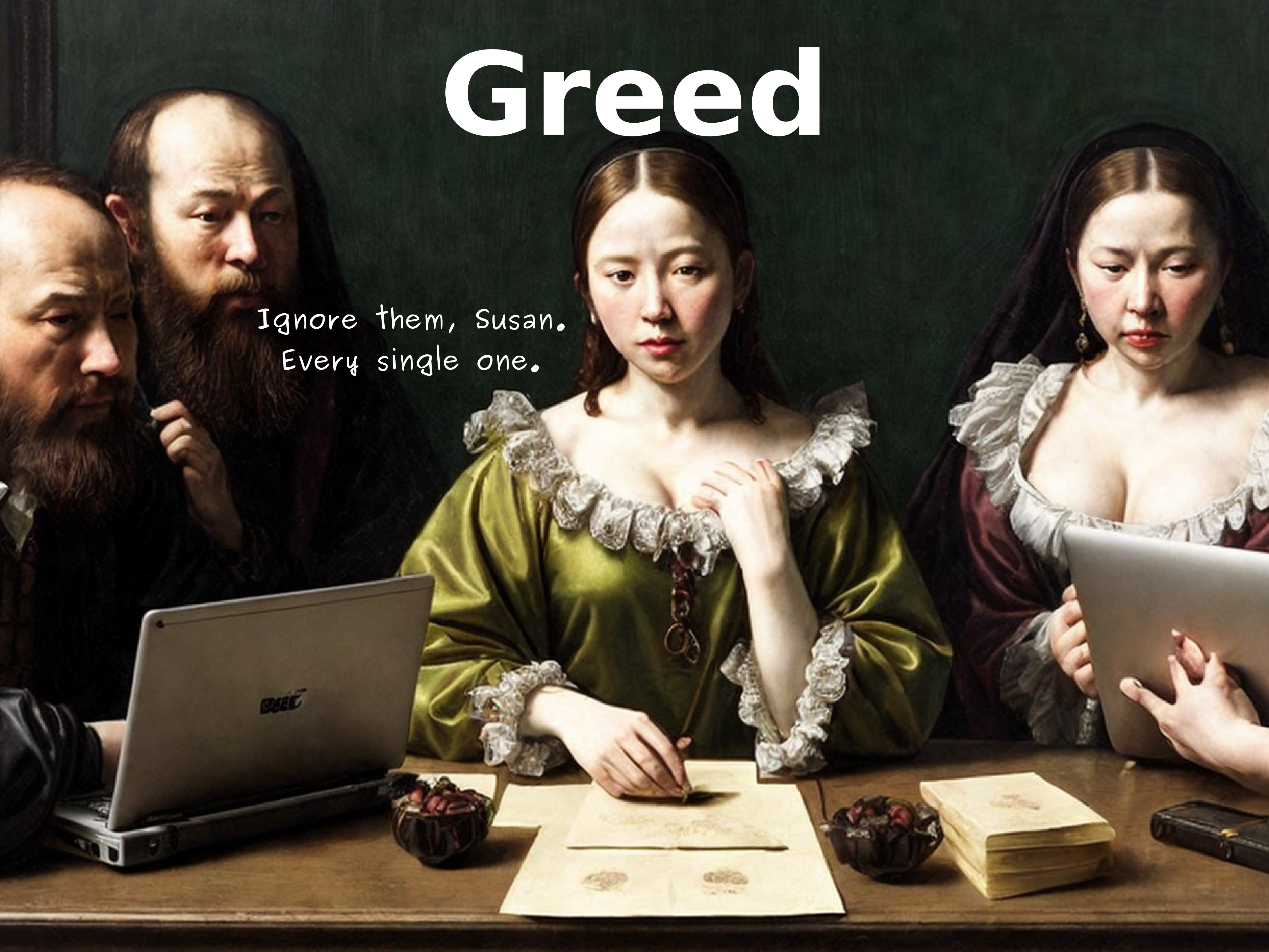


Greed



My lady,
The freelancers…
Have sent invoices

Greed



Ignore them, Susan.
Every single one.

Greed – or Avarice

- **The drive to achieve more profits or results at the expense of security.**
  - Cutting corners on security measures
  - Violating user privacy for monetary gain
  - Not investing enough into training
  - Believing there is one tool to fix it all
  - Believing that tools alone fix anything
- **Or the classic checkbox pentest.**
  - “We only need a quick scan, Nessus should do.”
  - “Hey we did something didn’t we?”

Sloth

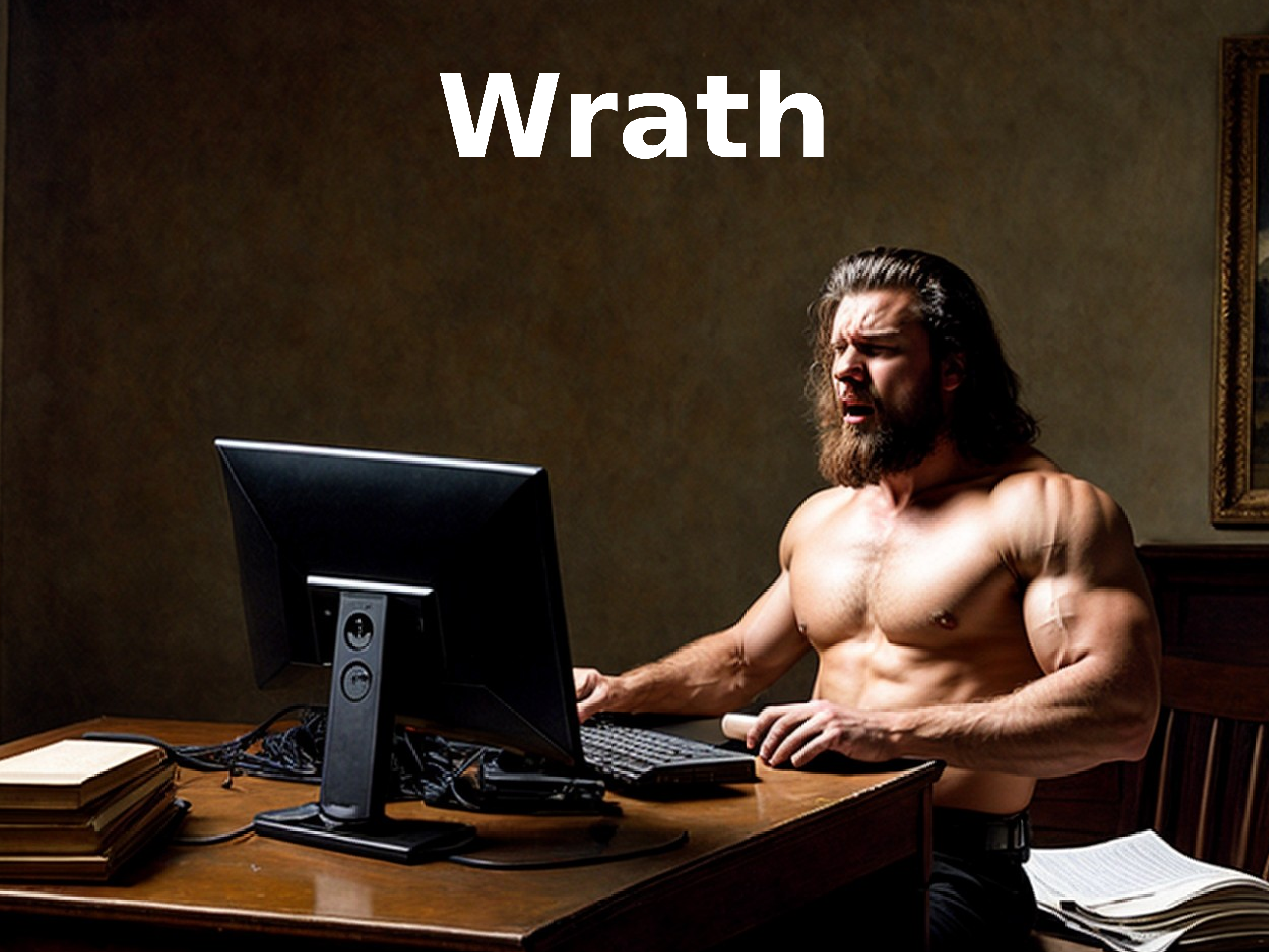
Sloth

Sloth

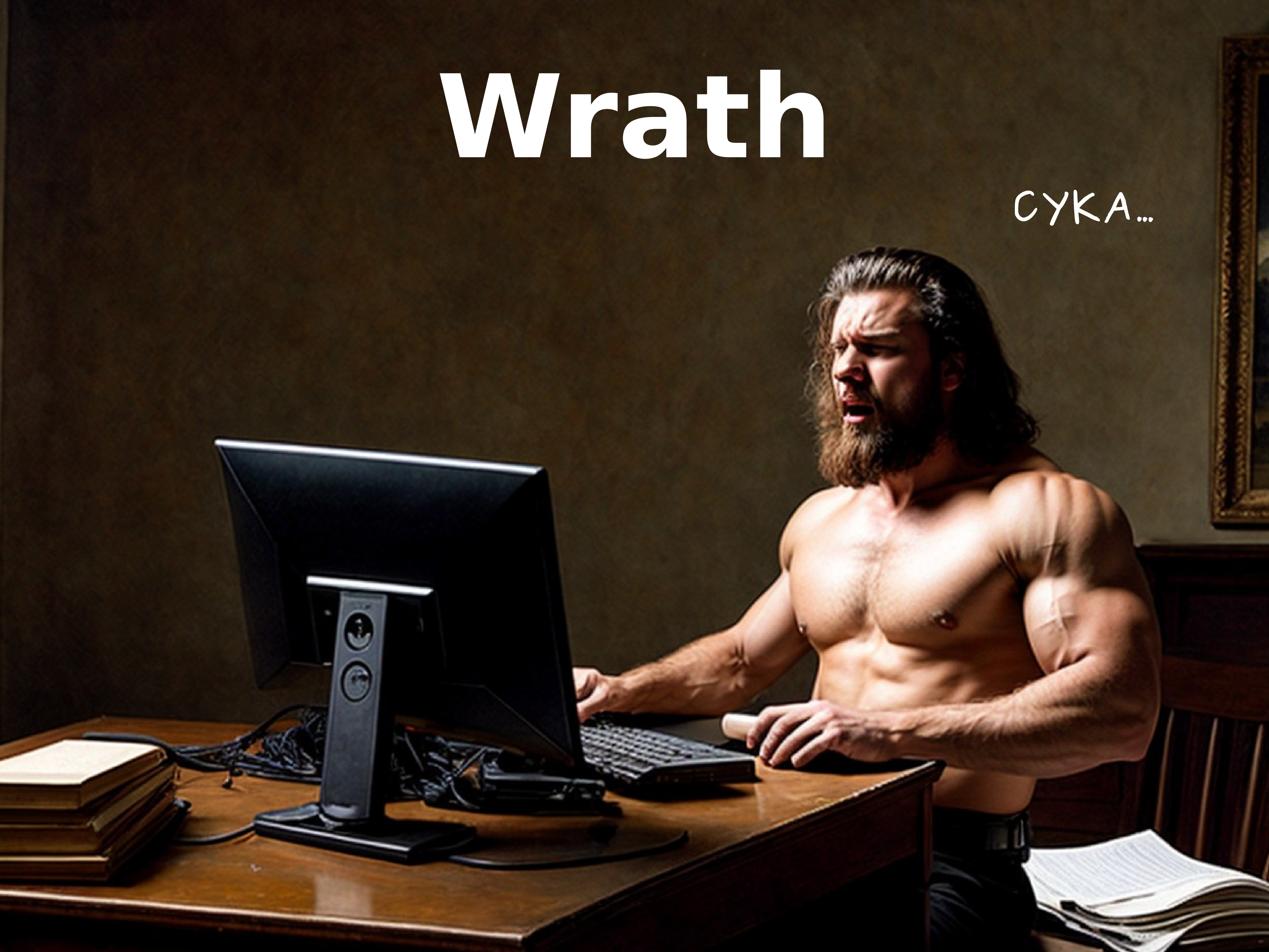
Sloth – or simply Laziness

- **This must be the classic, no?**
- **Lack of due diligence in maintaining systems, applying patches and updates**
  - Updates are annoying, never change a running system
  - We cannot update because the patched the core
  - Let’s maybe better not try to restart this system
- **Not following up on security news & alerts**
  - “Real men don’t read the news, real men *are* the news”
- **Complacency or inertia in improving outdated security best practices**
  - Of course all developers have root access to prod!
  - No one will ever guess the password is “123457”, genius!

Wrath



Wrath



Wrath

Wrath – or uncontrolled Anger

- **Often we see destructive behaviors in IT**
  - Denial of Service and DDoS come to mind
  - Such as for example like launching revenge cyberattacks
  - The insanely bad idea about hack-back
  - Or any other form of retaliation
- **Or engaging in harmful actions when a job is lost**
  - The disgruntled employee with too much knowledge
  - The politically motivated attacker with too much esprit
  - When IT and emotions blend, bad stuff must happen

Envy

Envy

at is he playing?

Envy

I think he is stuck in
some screensaver

Envy - or Jealousy

- **In a cyber-security context, this could manifest as industrial espionage**
  - Or insider threats, where individuals try to steal sensitive information from competitors
  - Or their own organizations out of jealousy or a desire to get ahead.
- **Or simply the idea that other folks have more to steal from**
- **And the illusion of not being an interesting target**

Pride

Oh!

Pride

My!

Pride

God
that sound
is awesome.

Pride - or Hubris

- **Overconfidence can be a significant issue in IT security.**
  - An organization might believe that its systems are secure and ignore advice or warnings to the contrary.
  - This could also manifest in a dismissive attitude toward end-user security training
  - Or a belief that security incidents "won't happen to us."
- **We have never been hacked before**
  - We don’t even read the logs anymore
  - That shell in the /tmp folder, um, we put it there to debug

Second Sermon

Seven Virtues

```
sudo apt update
sudo apt upgrade
sudo snap refresh
```

The Seven Virtues: Origins

- **Standing in stark opposition to the seven sins...**
- **We can find the seven virtues**
- **Written up in the 5th century, by Prudentius**
  - Chastity
  - Faith
  - Good Works
  - Concord
  - Sobriety
  - Patience
  - Humility
- **From Psychomachia, a poem about the battle between female personifications of virtues and the seven sins**

The Seven Virtues: IT Security

- **Chastity** - Use technology and data ethically and responsibly. Adhere to the principles of least privilege, maintain appropriate boundaries regarding data access and use.
- **Temperance** - Use a balanced approach to technology adoption, ensuring there's always a balance between security and functionality.
- **Charity** - Create and share secure code, contribute to the broader IT security community. Commit to user privacy and fairness in handling data.
- **Diligence** - Stay up-to-date with the latest security threats and defenses, regularly reviewing and updating security policies and procedures.
- **Patience** - Be patient with users and except them to make mistakes, educate them about good security practices instead of blaming them.
- **Kindness** – Treat users with respect and understanding, make systems and applications as user-friendly as possible while still maintaining security.
- **Humility** - Acknowledging that you don't know everything and that there's always more to learn in the rapidly evolving field of IT security.

2FA since 1760

A++ SSL Setup since 1761

Anything else?

Third Sermon

Path to Heaven

So what did we learn today?

- **Not much I guess, it’s a keynote after all**
  - We shall collectively hope that the **next talks** have more actual content
- **But we might understand parallels**
  - Old knowledge, **well matured**, applicable in new contexts
  - We can remove the religious context and start seeing the seven sins for what they represent
  - As well as the seven virtues. **Improvement**.

Small Steps

Let’s start with ourselves

Small Steps. But Steps.

- **No one can become a better human just so**
  - It takes lots of time and work, it’s always an uphill battle
  - And nobody is perfect. No one is.
  - If someone seems perfect, be sure they just wear their mask well.
  - At the end of the day, no one has their sh*t together.
  - No one does.
- **But we can make small steps here and there and learn, enhance, adopt, improve**
- **And an event like this is where it happens.**

To Sum Up

- **Let’s digest that ancient knowledge and see how it holds today**
- **Let’s see what we can do to constantly push towards betterment**
- **Let’s use this and other events to learn, get inspired and progress**
- **Let’s make things more secure together!**

Amen!

- **Many thanks to y'all!**
  - **Got any questions?**
    - mario@cure53.de
- **Thanks also go out to...**
  - The BSides Orga Team
  - Stable Diffusion
  - ChatGPT-4