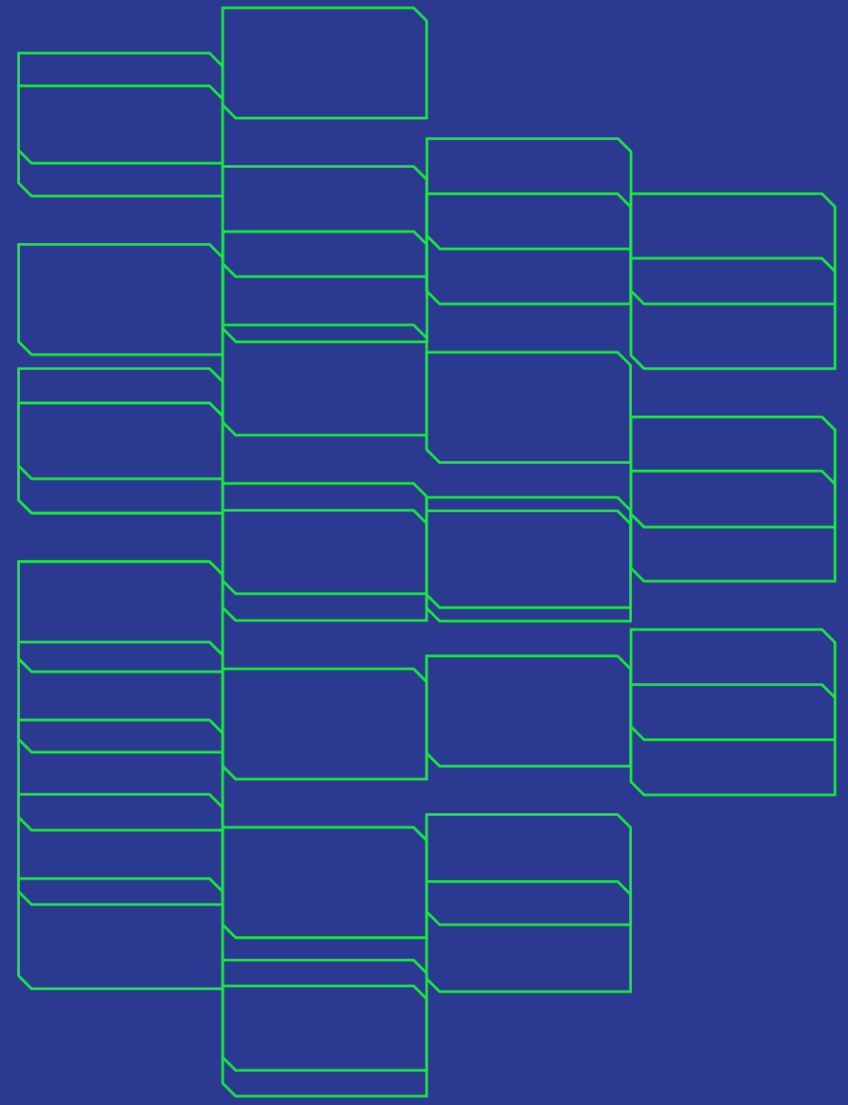
Security .Days

<Utrecht.NL>
<7-9 April 2026>

GÉANT

Building a cybersecurity capability from scratch in Academia

Łukasz Faber



Co-funded by the European Union

AGH

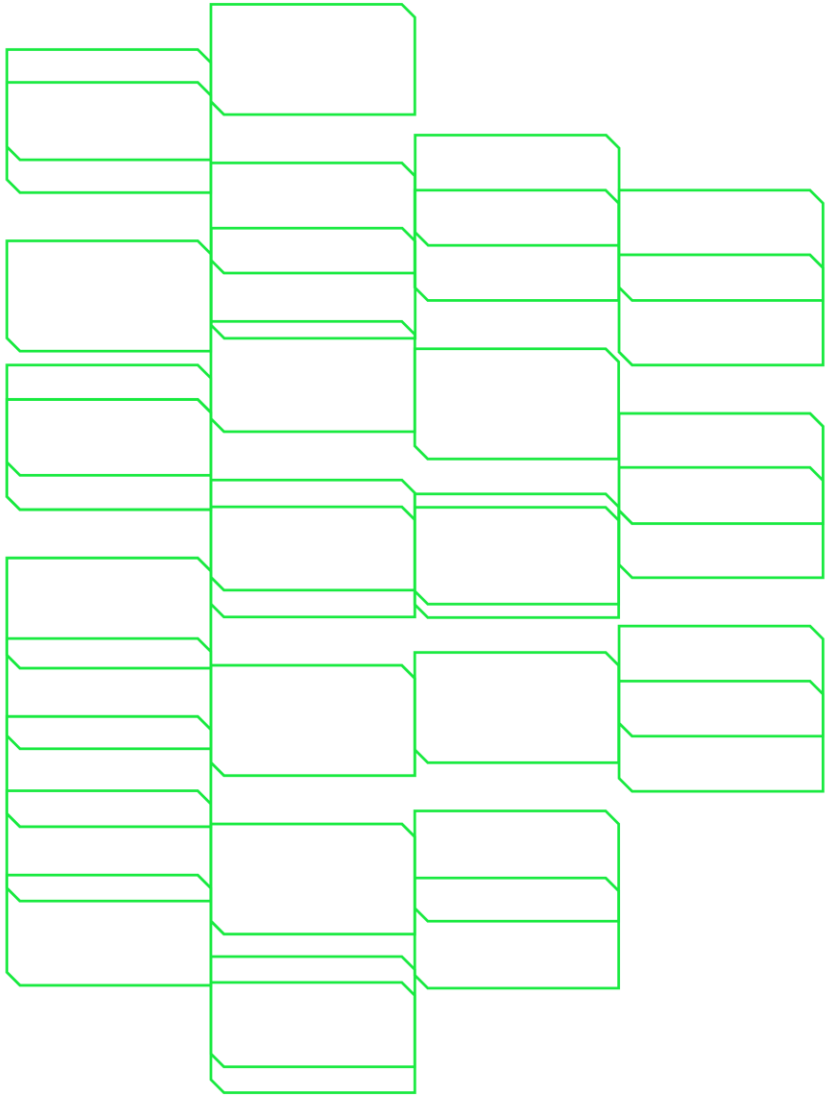
Centre for Information Security

AGH University of Krakow

- Technical university
- Over 100 years
- 18 faculties (like small companies)
- Countless administrative departments
- Almost 20 000 students and nearly 2000 postgraduate students
- Over 4,500 staff members (counting FTE only)

Academia uniqueness

- Openness culture
- A wide range of stakeholders
- Limited (mostly financial) resources
- Decentralised management




WAKE UP SAMURAI
WE HAVE A CYBERSECURITY
CAPABILITY TO BUILD

We started with…

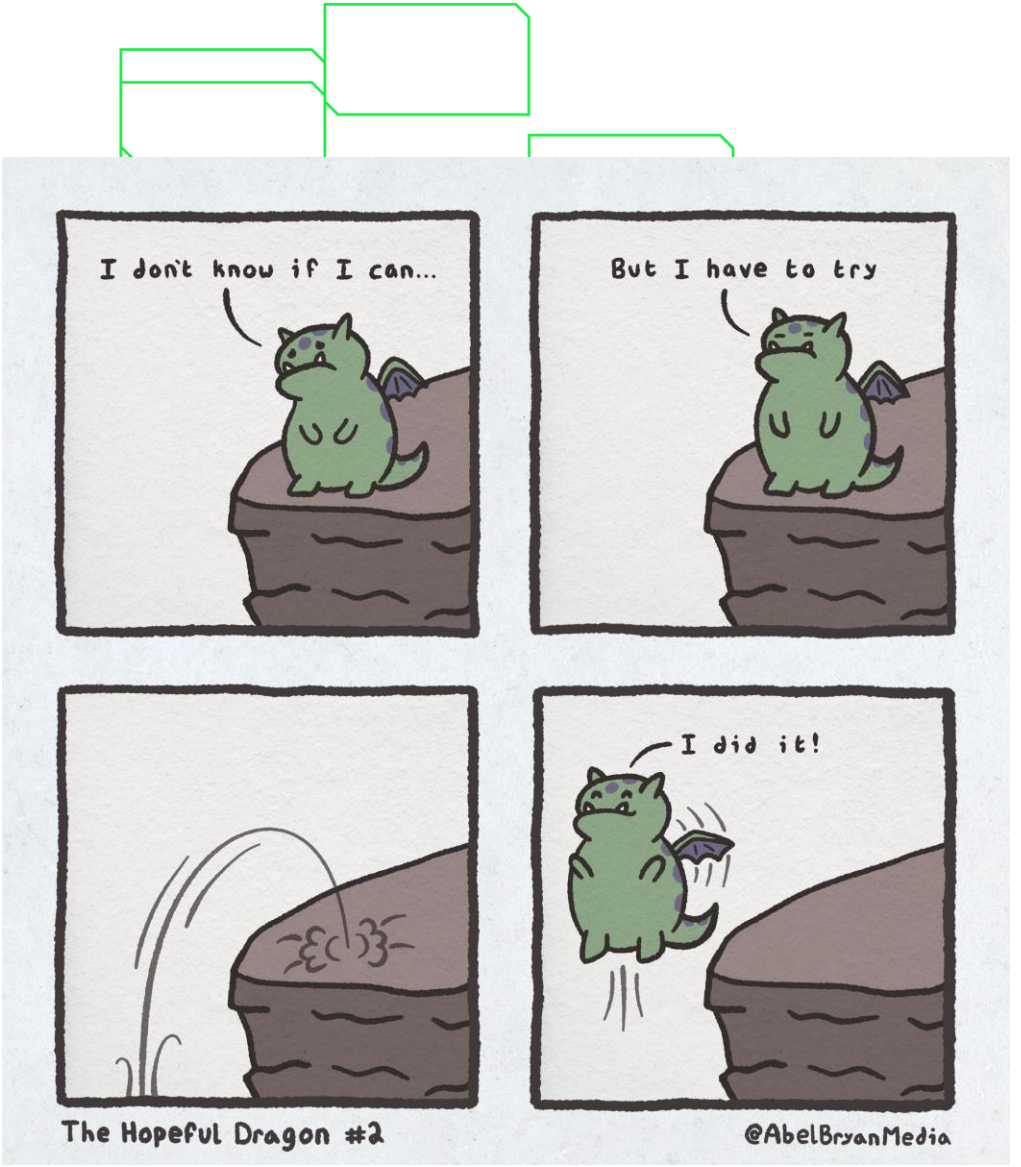
- Good but “opinionated” IT
- No separate security function
- Scattered monitoring
- Scattered responsibilities
- Scattered ownership
- Local information security administrators
- No awareness building
- Risk management… having issues
- Lack of understanding of what is needed for security processes to function

Then we set goals…

- A more ‘state-of-the-art’ approach to security
- A team covering all practices comprehensively
- A shift in the way information security is managed
- A strong link to academic research
- Providing external services

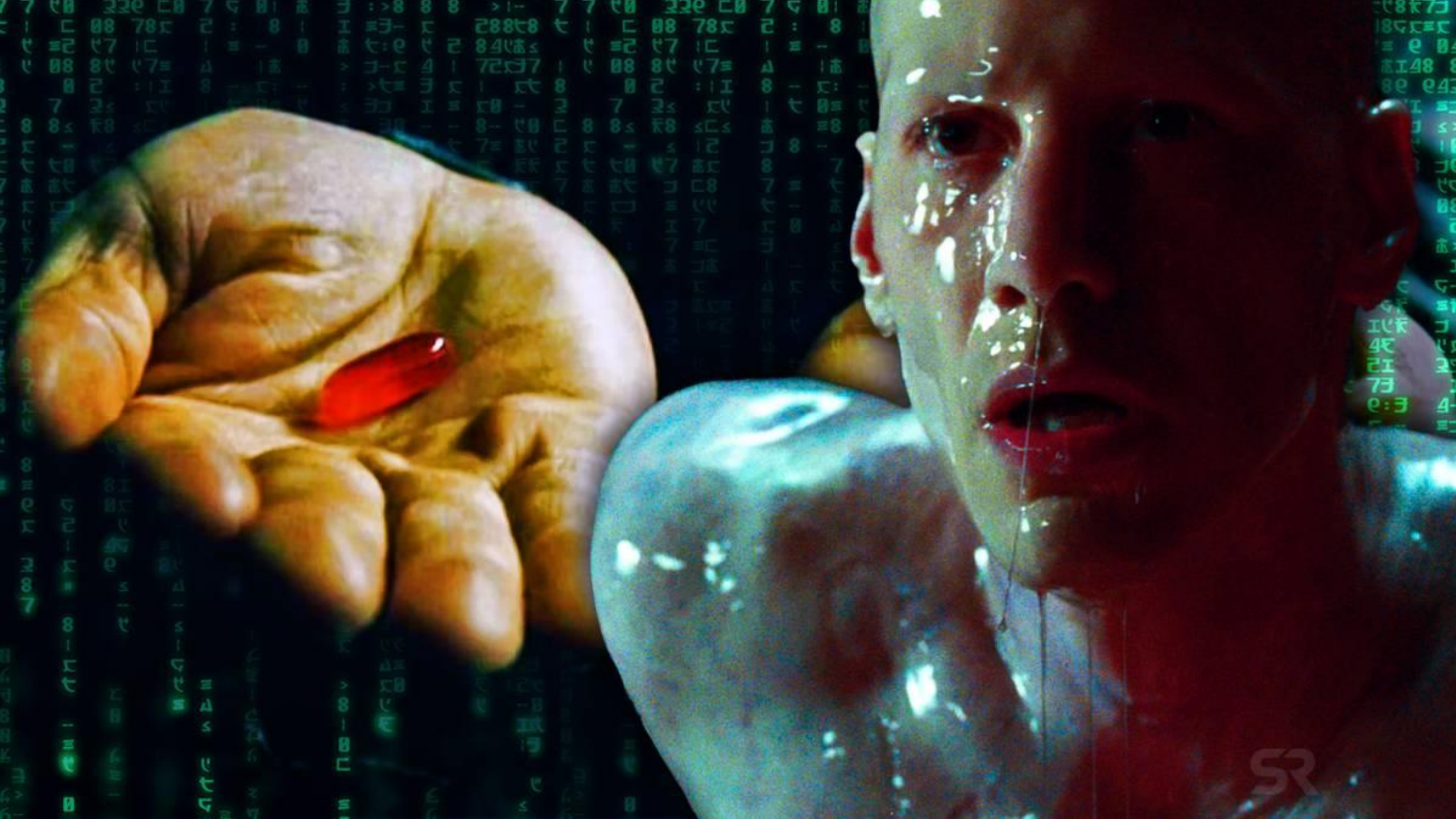
Then we made a plan and started working…

- Two people at the beginning
- And a hopeful timeline of one year



And then…

- Management support
- IT happy that they can do less
- Budget for everything
- Changes welcome and easily introduced



In reality…

- Management does not even remember you
- IT hides incidents from you
- You can buy anything if you find money outside
- You can deploy anything as long as it won’t be doing anything
- And no one even understands why you are needed

Timeline

And in 2026 we are large enough to develop an internal structure…

And now some insights…

Hiring

- People from outside, not internal recruitment
- Broad and wide knowledge especially for the first employees
- Students are ok, but ethics and conflict of interest issues arise
- For SOC, we went with untiered model
- We've made some mistakes, but in general most of our choices were great

Team development

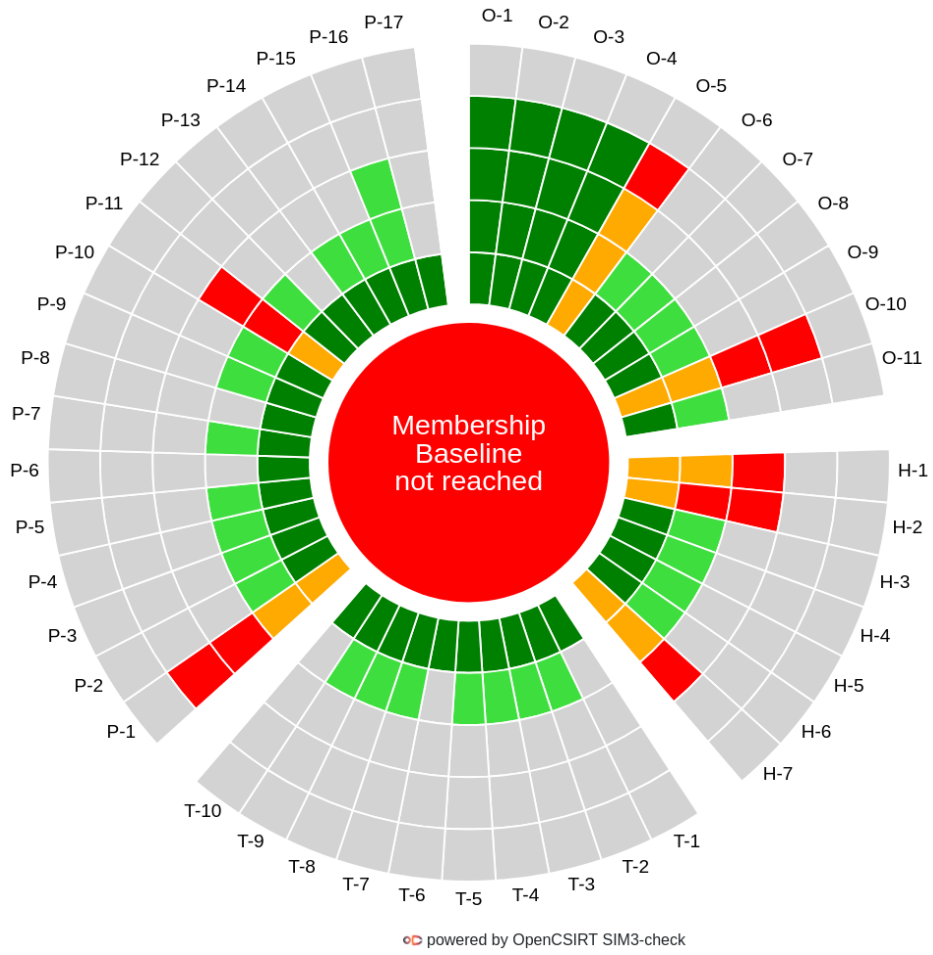
- We match our team to European Cybersecurity Skills Framework
  - https://mta-sts.enisa.europa.eu/ECSF/
- Whole SOC Staff went through BTL2 and a basic forensic training
- CTFs and similar are encouraged
- Freedom to participate in responsibilities and projects outside normal scope

Some of our tools & resources

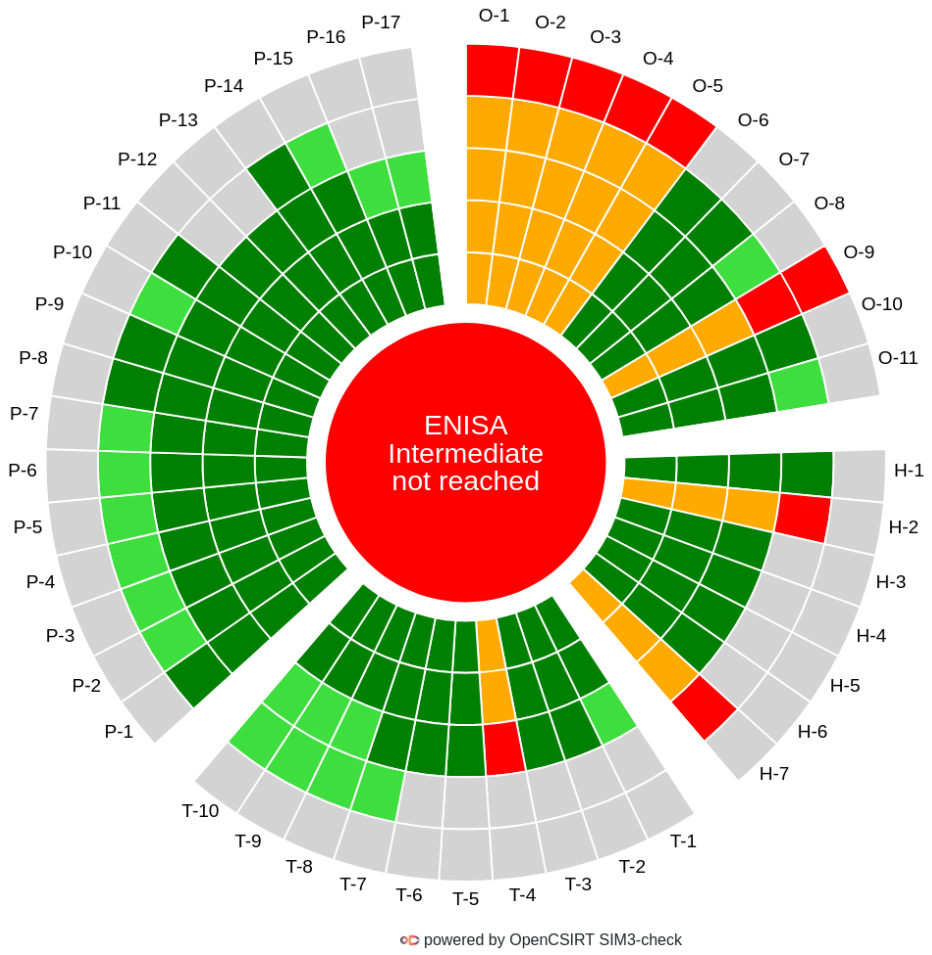
- SIEM – initially went with well-known American brand, now evaluating national and open-source solutions
- Surface management – Nessus, Shodan, moje.cert.pl
- Vulnerability management – Nessus, DefectDojo
- CTI – ShadowServer, Connect2Trust

SOC Maturity

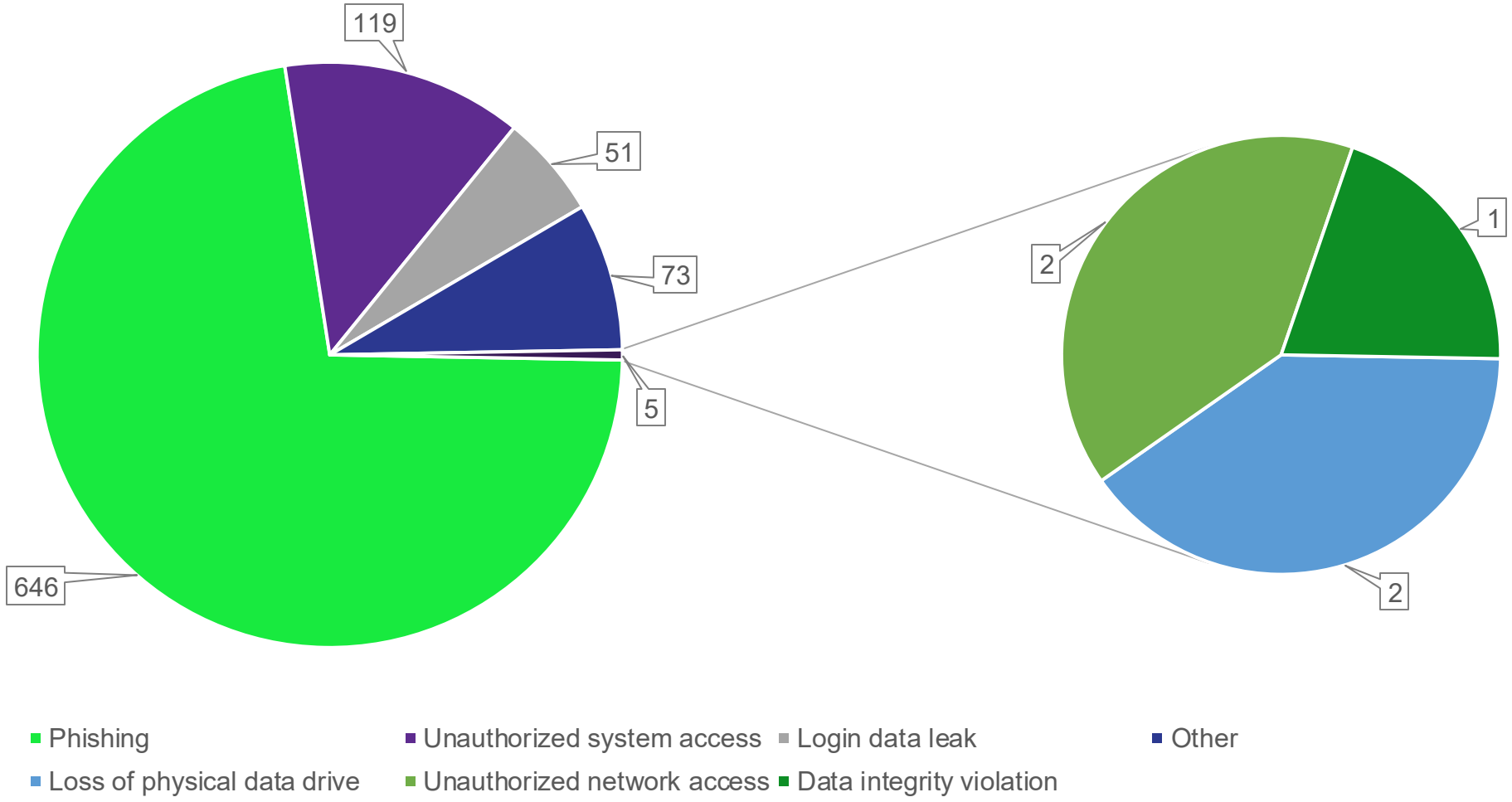
Starting point



18 months



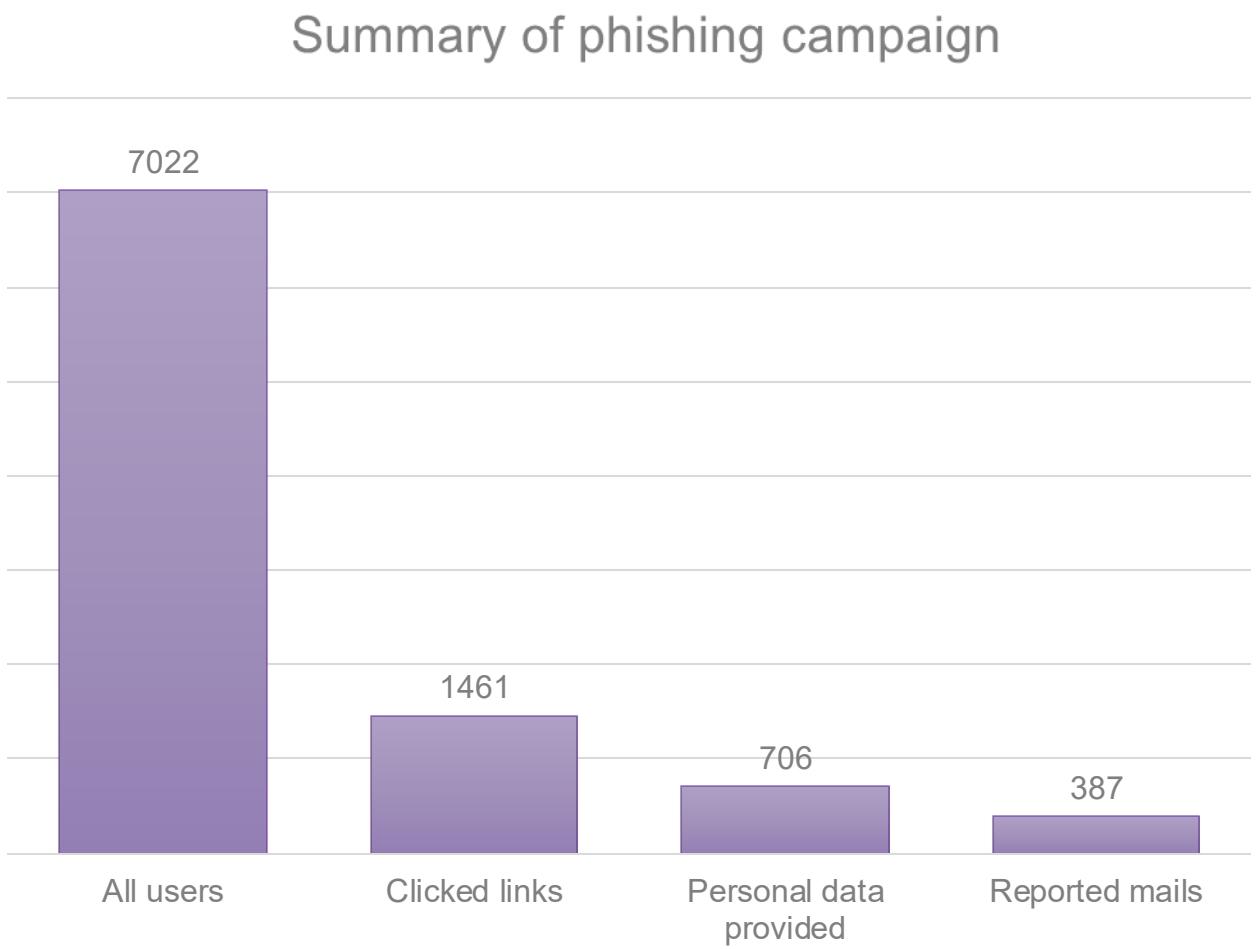
Incidents in 2025



Awareness training

- First ever cybersecurity awareness trainings for employees and students
- „Cyber-secure work at AGH!”
  - Real fundamentals of IT and data security
  - Authentication
  - Remote work
  - Phishing & malware
  - Incident reporting
- 43% of faculty and staff finished the first (voluntary) edition
- Phishing campaigns

First ever phishing campaign



[EXT] Weryfikacja danych logowania

AP AGH Powiadomienia <noreply@agh.edu.pl>
Do Wojciech Kiełb

W przypadku problemów ze sposobem wyświetlania tej wiadomości kliknij tutaj, aby wyświetlić ją w przeglądarce sieci web.

Dzień dobry,

W związku z wejściem w życie **nowych przepisów od 1 stycznia 2026 roku**, informujemy, że dotychczasowe poświadczenia logowania do usług pocztowych **mogą utracić ważność**.

Aby zapewnić nieprzerwany dostęp do Poczty AGH oraz dostosować konto do zaktualizowanych wymogów bezpieczeństwa, konieczne jest przeprowadzenie **jednorazowej weryfikacji danych logowania**.

Prosimy o kliknięcie poniższego przycisku, który przeniesie na stronę umożliwiającą potwierdzenie danych logowania:

Przejdź do weryfikacji

Link jest **jednorazowy** i pozostaje aktywny przez okres **7 dni** od momentu otrzymania wiadomości.

Brak potwierdzenia danych może skutkować **czasową blokądą dostępu** do skrzynki pocztowej do czasu ręcznego potwierdzenia tożsamości.

Z poważaniem,
Sekcja Wsparcia Użytkowników

Wiadomość została wygenerowana automatycznie. Prosimy na nią nie odpowiadać.

Application security

- AGH produces a lot of internal and external software
- How to convince developement teams that they need SSDLC?
- Legwork, presentations
- In 2025 alone, 17 applications were tested
  - Including these bought from external provider

Biggest challenges (up to today)

- Cooperation with central IT
- Reworking risk-management
- Working without backing policies
- Navigating internal politics
- Integration of security into processes (like vendor management)
- Underestimation of time needed for changes in Academia

Why just not outsource?

- Universities are quite unique
- Everyone sells „NIS 2 ultimate solver” nowadays which gives false sense of security
- It would be easier, but no value for the academia mission

What was important?

- SOCCER project
- ECSO membership
  - https://ecs-org.eu/
- Very good cooperation with some key players: DPO, Rector’s office
- Great team

About the SOCCER project

SOCCER

- SOCCER – Security Operation Centre in Central-Eastern Europe Region
  - https://soccer.agh.edu.pl/
- Main objectives of the project:
  - Supporting the creation of SOCs or readiness to have them in participating universities
  - Creating the SOC4Academia Toolbox (instructions on how to create SOC in Academia)
  - Creating a threat intelligence sharing ecosystem (CTI) for the academic community

What don't we have?

- 24/7 SOC – only regular working hours
- Widespread monitoring in faculties – requires more resources and some coercion
- Integrated physical security – a siloed responsibility area

Where are we standing?

- Over 20 employees in the security capability alone
  - SOC, AppSec, Pentesting, GRC, Training and awareness
- Just days before new ISMS
- Helping other universities (as NIS 2 implementation in Poland included universities as a essential/important sector)
- 7 DEP and Horizon grant applications with strong consortia

What was important?

- You cannot just act as a service provider but as a partner in research actions
- You need sympathetic and forgiving staff
- People-oriented approach: valuing individuals, fostering teamwork, and prioritizing team building

Biggest challenges in future?

- Being noticed by management
- Balancing tight budgets with big cybersecurity ambitions
- Keeping up with IT updates before they update us first
- Chasing cyber threats faster than students find new ways to break the rules
- Turning alerts into actions before coffee runs out
- Running a university SOC... and staying sane

Thank you!

faber@agh.edu.pl
https://www.linkedin.com/in/faberlukasz/

Co-funded by
the European Union