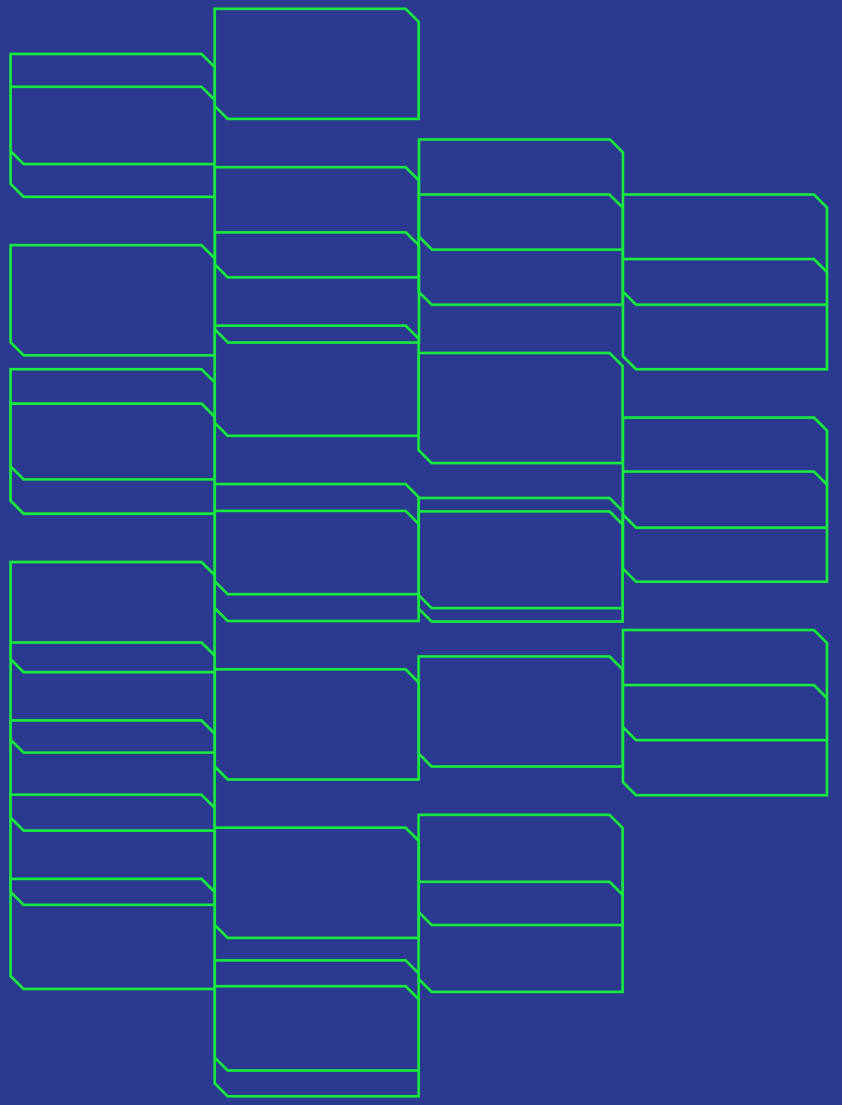
Security .Days <Prague.CZ> <9-11 April 2024>

Security of bespoke solutions vs academic curricula

Maciej Miłostan, PhD, (ISC)2 SSCP
PSNC and PUT

Co-authors: Mikołaj Dobski, Gerard Frankowski



Co-funded by the European Union

About myself

Maciej Miłostan, PhD
(ISC)2 Systems Security Certified Practitioner

30 YEARS OF POZNAŃ
SUPERCOMPUTING AND NETWORKING CENTER

- Two main hats:
  - PSNC (since 2003):
    - Member of ICT Security Department (Security Team in short)
    - Rep. of PIONIER-CERT team (TI accredited)
    - GN5-1 WP8 T3-4-CTI plus support of SCT (Secure Coding Training) activities within WP9
    - R&D Projects (Threat Modelling, decision aiding etc.)
  - PUT (since 2000):
    - IT infrastructure administration at Computing Science Institute
    - Teaching activities (security and programming)
- Other activities
  - Cybersecurity @ University Merito in Poznań

Introduction to the problem

Projects and resources

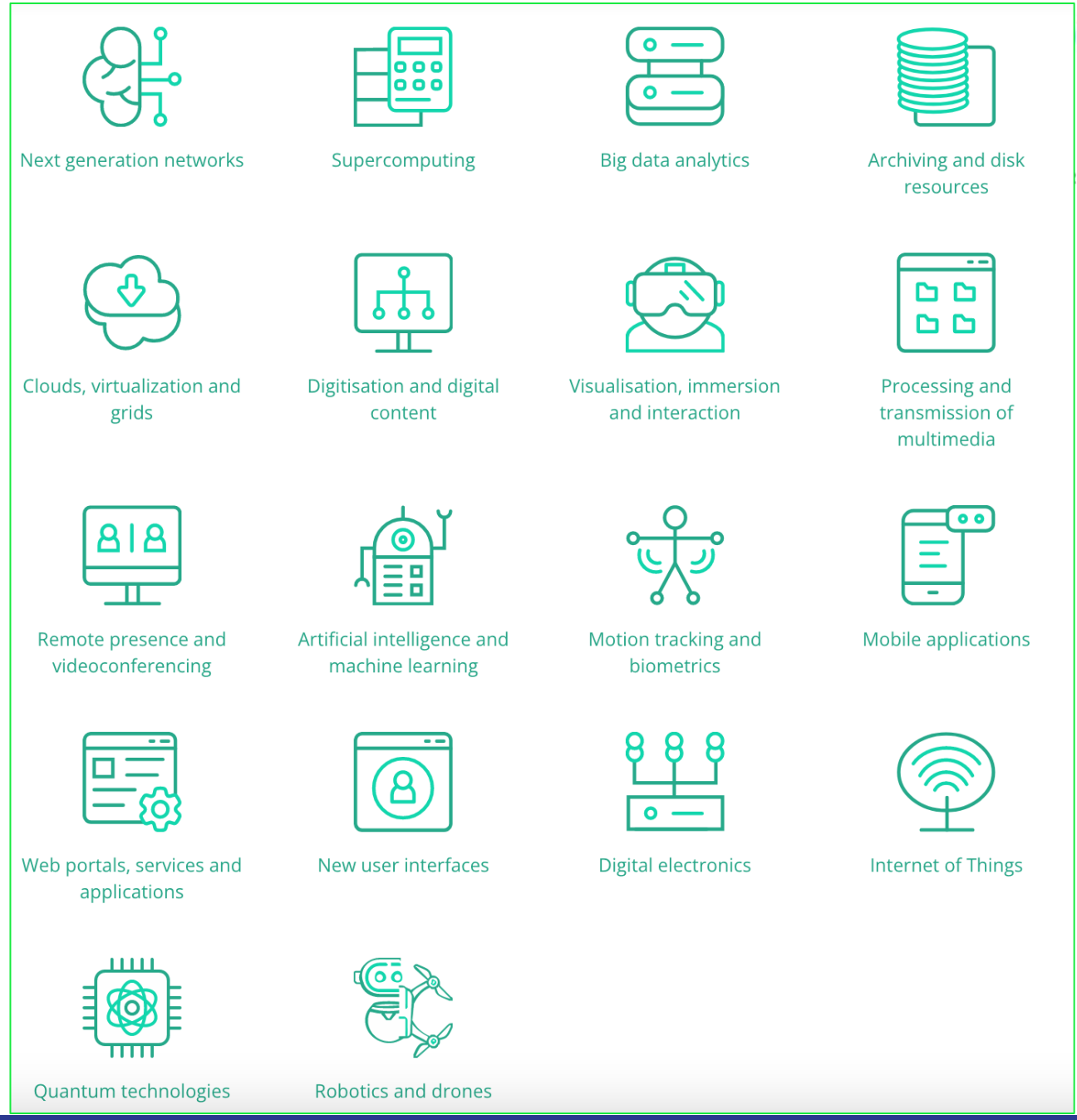
Security team @ PSNC

30 YEARS OF POZNAŃ SUPERCOMPUTING AND NETWORKING CENTER

- Security team conducts:
  - code audits,
  - pen-tests,
  - threat modeling,
  - trainings
  - and more ☺

R&D Projects

- Diverse portfolio of project and activities @ PSNC
- No off the shelf solutions
- Limited number of functionalities available out of the box
- Bespoke (custom) software is a must



Projects and resources

30 YEARS OF POZNAŃ
SUPERCOMPUTING AND NETWORKING CENTER

Projects to be done and code ☺

Money we have

Projects and resources

30 YEARS OF POZNAŃ
SUPERCOMPUTING AND NETWORKING CENTER

Projects to be done and code ☺

Money we have

We need fresh mates / juniors!

30 YEARS OF POZNAŃ
SUPERCOMPUTING AND NETWORKING CENTER

Projects to be done and code ☺

Junior Staff
(AI generated)

We need fresh mates / juniors!

30 YEARS OF POZNAŃ
SUPERCOMPUTING AND NETWORKING CENTER

Projects to be done and code ☺

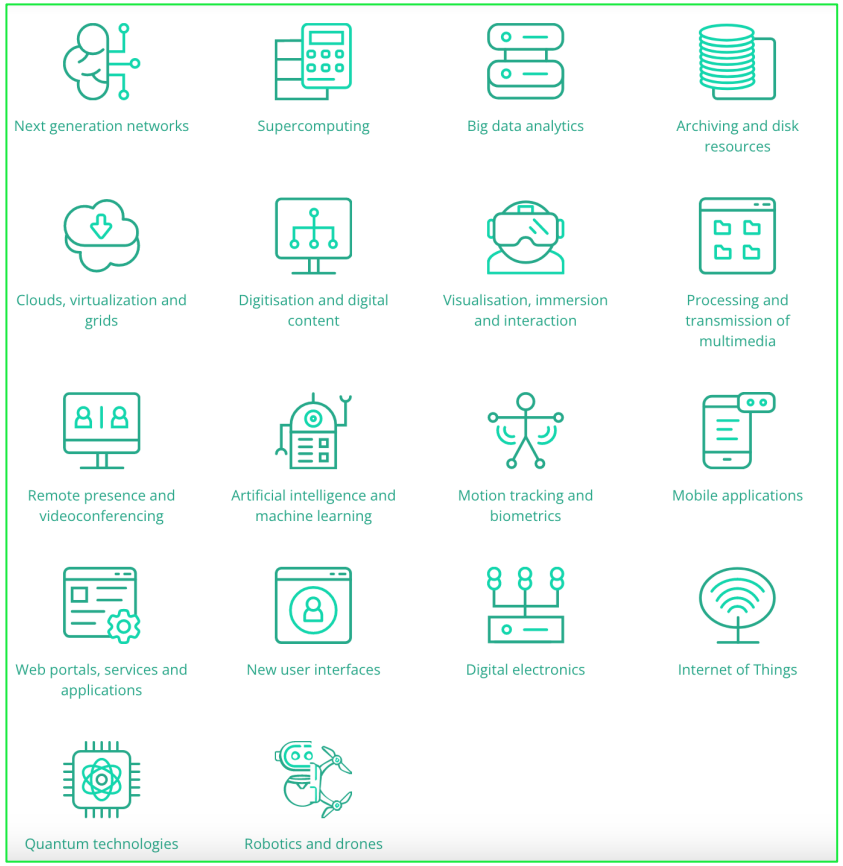
Junior Staff
(AI generated)

We need fresh mates / juniors!

Projects to be done and code ☺

Junior Staff
(AI generated)

We need juniors (and seniors as well)



Projects to be done and code ☺

Junior Staff
(AI generated)
+ experienced ~~master~~ senior

The problem

How to develop secure software with limited resources?

The problem

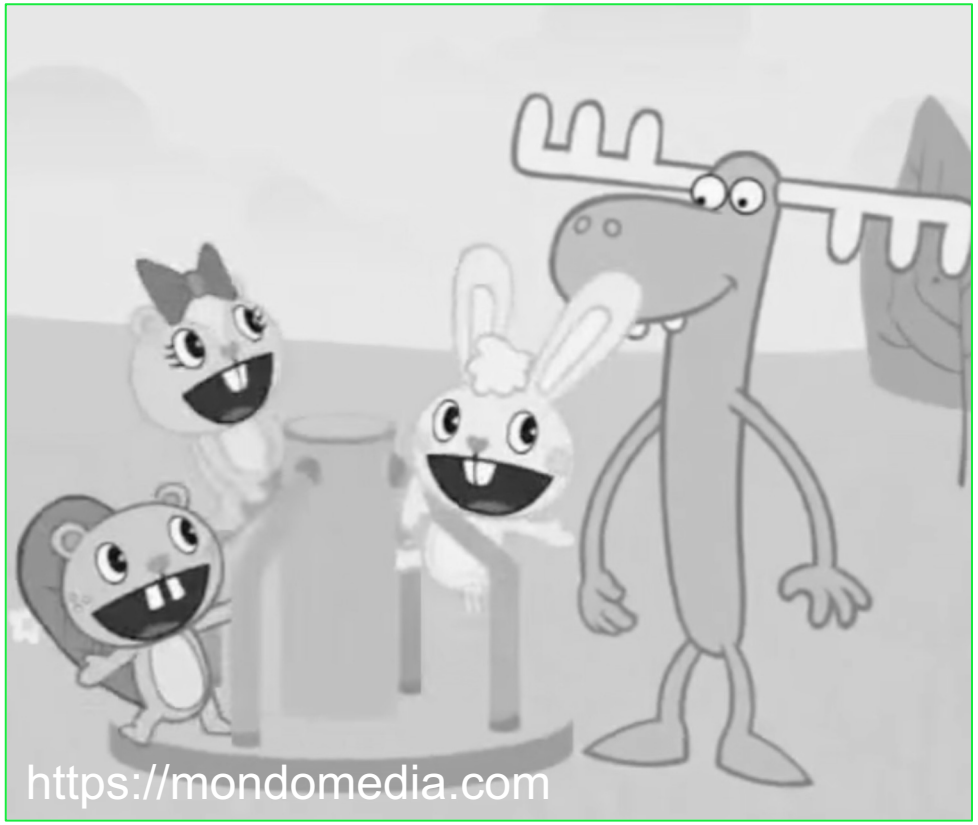
30 YEARS OF POZNAŃ
SUPERCOMPUTING AND NETWORKING CENTER

- Entry data
  - Team
    - A team of (mostly) gifted by not experienced programmers (only a few seniors)
    - with different backgrounds and education paths, and
    - with growing financial expectations (one of the reasons of leave and rotations)
  - Projects
- Goal
  - Secure software
  - Happy team!

Frequent rotation vs software quality

30 YEARS OF POZNAŃ
SUPERCOMPUTING AND NETWORKING CENTER

- We want to keep our junior employees in the team (at least happy)
- But we can’t afford to keep them all
- We want to provide high level of software ~~quality~~ security



How to build secure software?

30 YEARS OF POZNAŃ
SUPERCOMPUTING AND NETWORKING CENTER

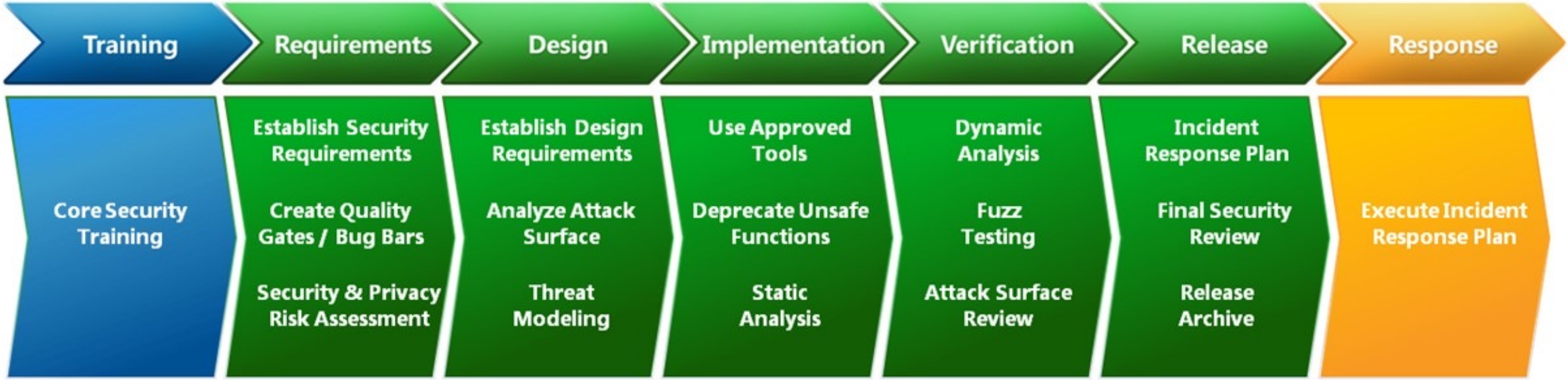
- Mentoring and well defined software development processes
- Make programmer a team player
- Educate your employees
- Know what your employee knows and fill the knowledge gap

Do not leave your staff alone

SDL(C)

30 YEARS OF POZNAŃ
SUPERCOMPUTING AND NETWORKING CENTER

We cultivate the adoption of the Microsoft Security Development Lifecycle within the projects whenever possible.



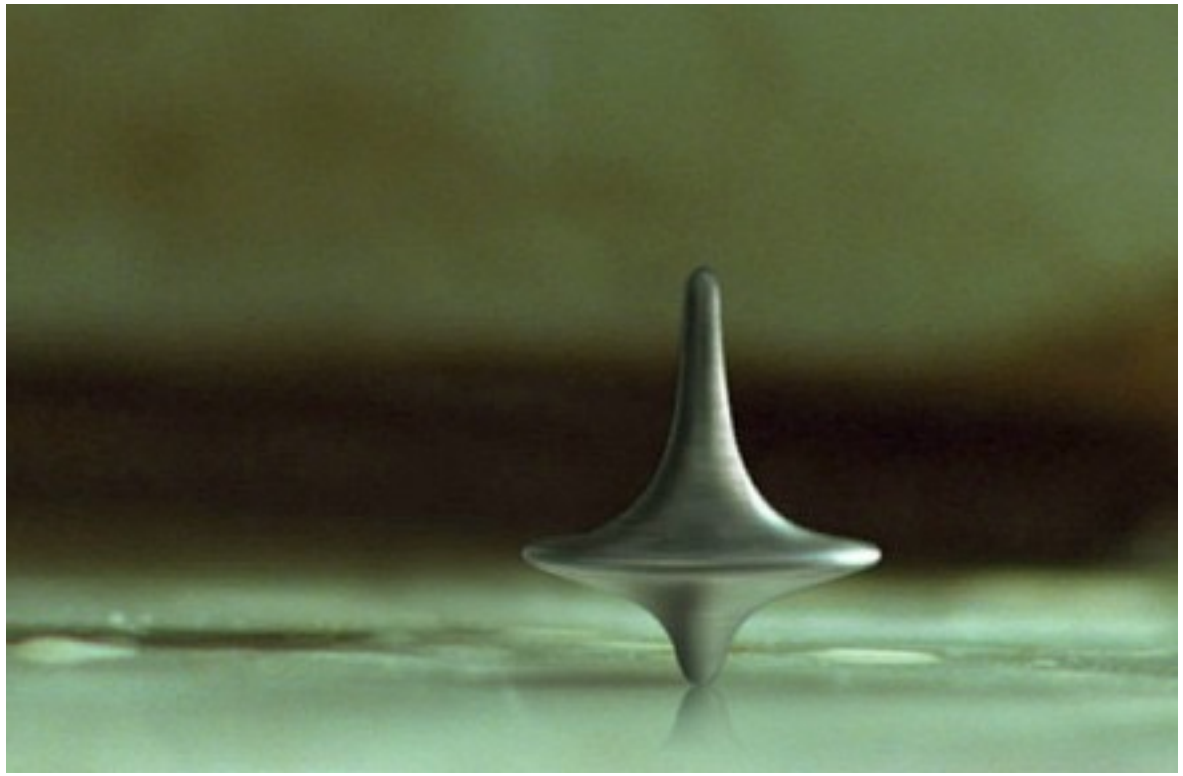
The knowledge gap

Do developers know enough about SDLC?

The reality

30 YEARS OF POZNAŃ
SUPERCOMPUTING AND NETWORKING CENTER

- Let’s make a step back
- Are we all (especially programmers and security team) in the same universe?
- What knowledge and skills should we expect from graduates (or even students) in general?



What do junior staff know?

30 YEARS OF POZNAŃ SUPERCOMPUTING AND NETWORKING CENTER

Programming principles?

Data structures?

Basic algorithms (e.g. sorting, branch & bound, meta-heuristics)?

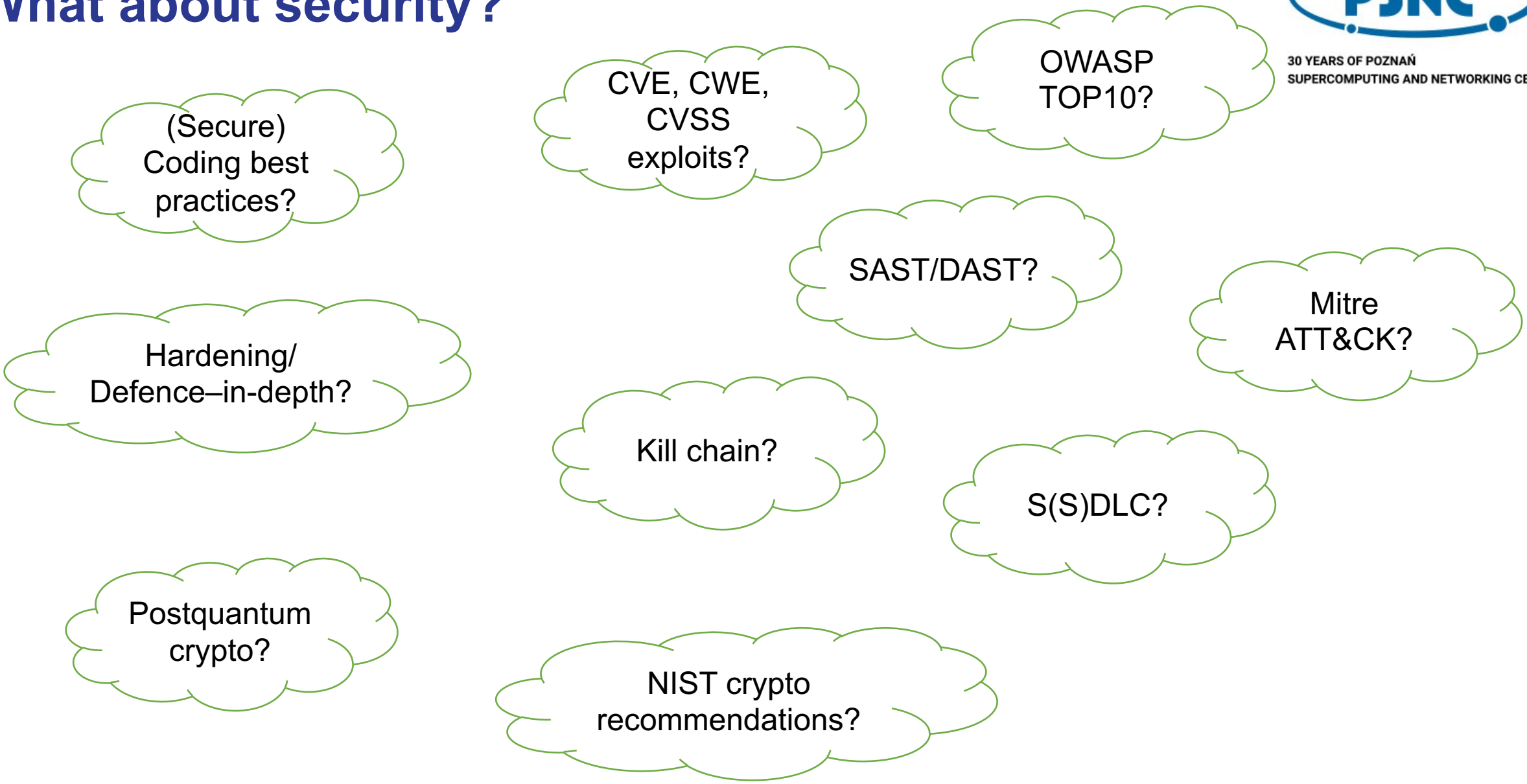
AI/ML algorithms?

It depends!

IDE, compilers, dev tools?

Principles of cryptography?

What about security?

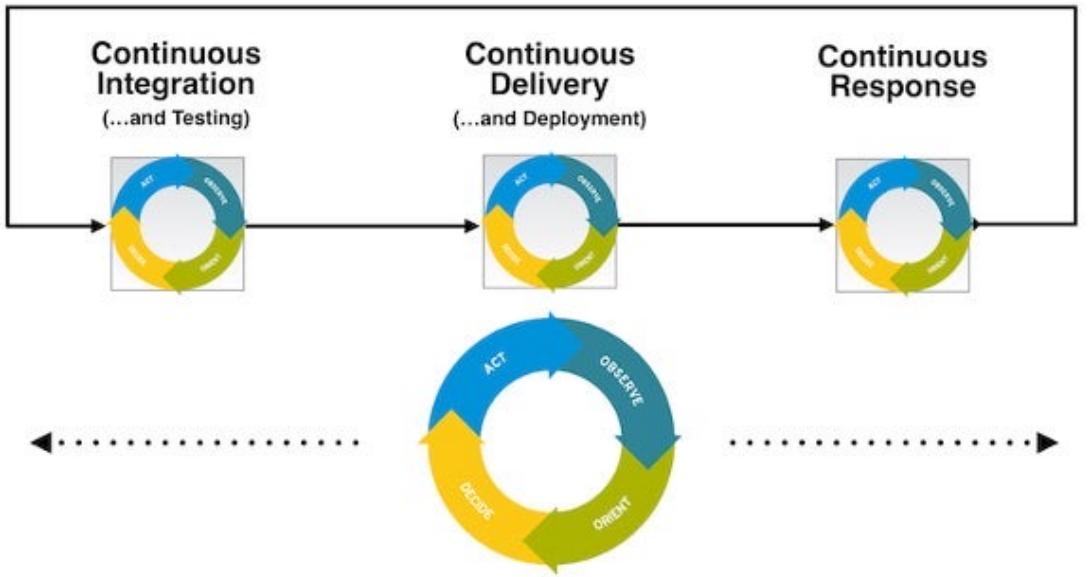


30 YEARS OF POZNAŃ SUPERCOMPUTING AND NETWORKING CENTER

What about DevOps / SystemOps skills?

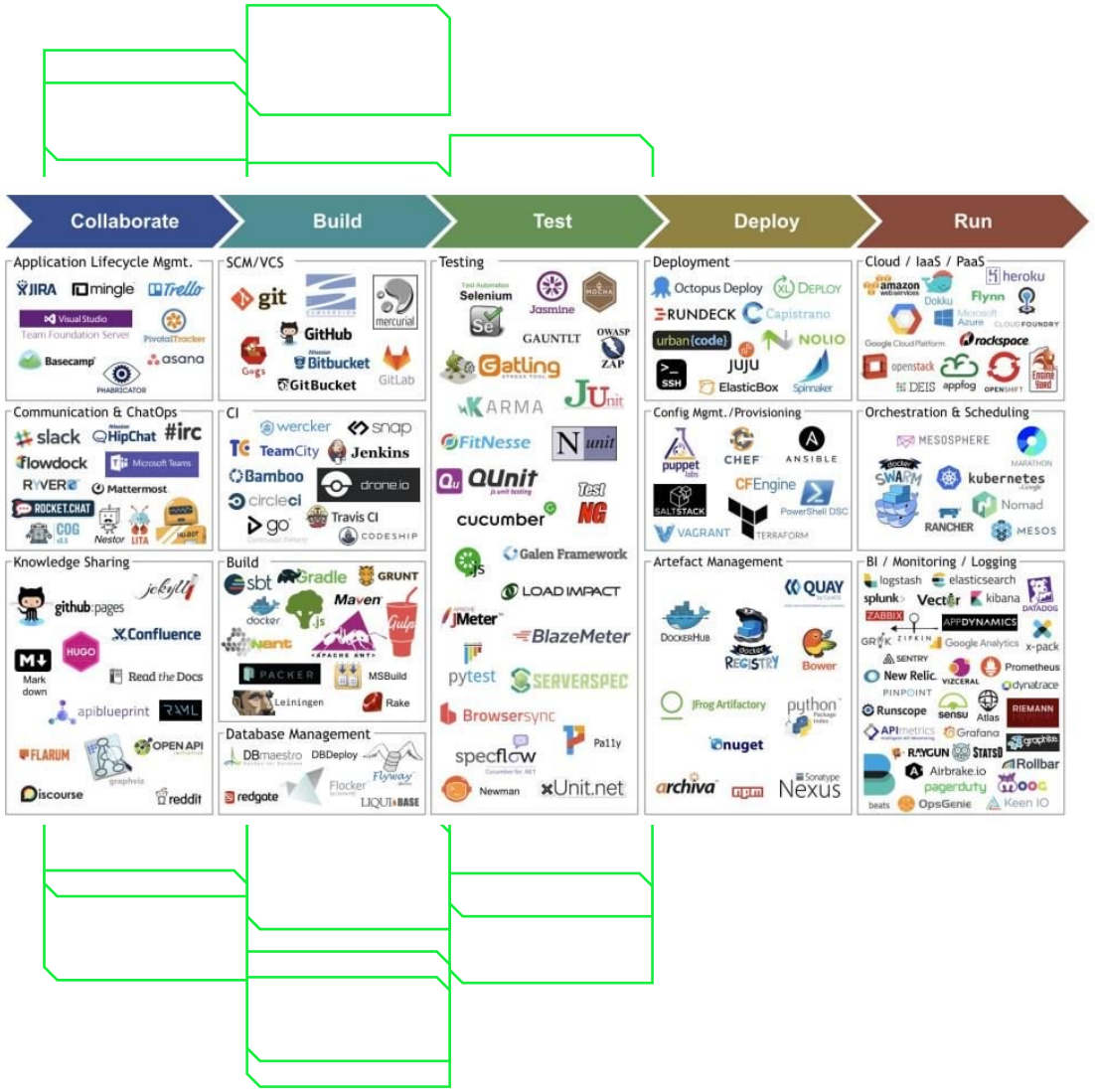
30 YEARS OF POZNAŃ SUPERCOMPUTING AND NETWORKING CENTER

- System management and automation skills
  - Virtualization
  - Containerization
  - Collaborative platforms (usage and setup)
  - System Configuration and Hardening
- Basic skills
  - SSH, git
  - Secure access (VPN, IP forwarding)



Holistic DevOps Cycle

What about newest technologies?



- Continuous / Self learning
  - building the learning skills
  - analytical / educational Fridays
- Internal courses
- Access to training platforms
- Building problem solving skills

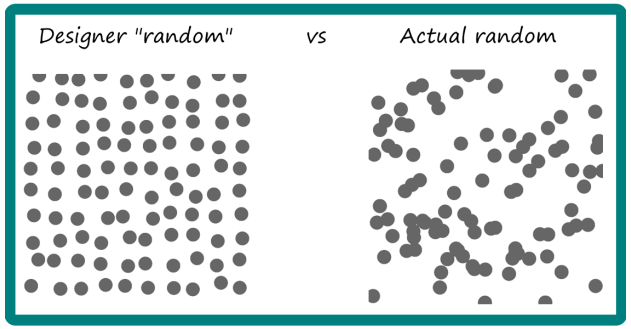
Feedback from the audits

What does need improvement and possible emphasis in academic curricula?

Feedback from software audits and pen-tests

30 YEARS OF POZNAŃ SUPERCOMPUTING AND NETWORKING CENTER

- Feedback comes not only from internal projects – we are doing also external audits
- Software audits
  - Inappropriate input validation
  - Lack of /Poor encryption
  - Lack of randomness
  - Insecure randomness
  - OWASP TOP 10 never dies
- Pen-tests
  - Same as code audits plus
  - Outdate software
  - Exposed services
  - Problems with external dependencies



What to do?

Let’s put some more security in academia and universities

What to do to limit the security knowledge gap?

30 YEARS OF POZNAŃ SUPERCOMPUTING AND NETWORKING CENTER

- Within GÉANT community
  - Let's keep providing and socialize available complimentary education:
    - Secure Coding Training
    - Summer School of Software Engineering
    - Expand portfolio of GLAD courses
  - Let's provide access to quality pen-tests and code audits (e.g. cross checks within the community)
  - What about organizing CTFs / Hackathons?
- Outside the community
  - Engage in preparation of curricula for CS / AI students
  - Promote usage of best practices
  - Influence decision makers
  - Provide complimentary courses, especially around emerging technologies
  - The voice of the security community should be heard

Any questions?

Email: milos@man.poznan.pl

Co-funded by
the European Union