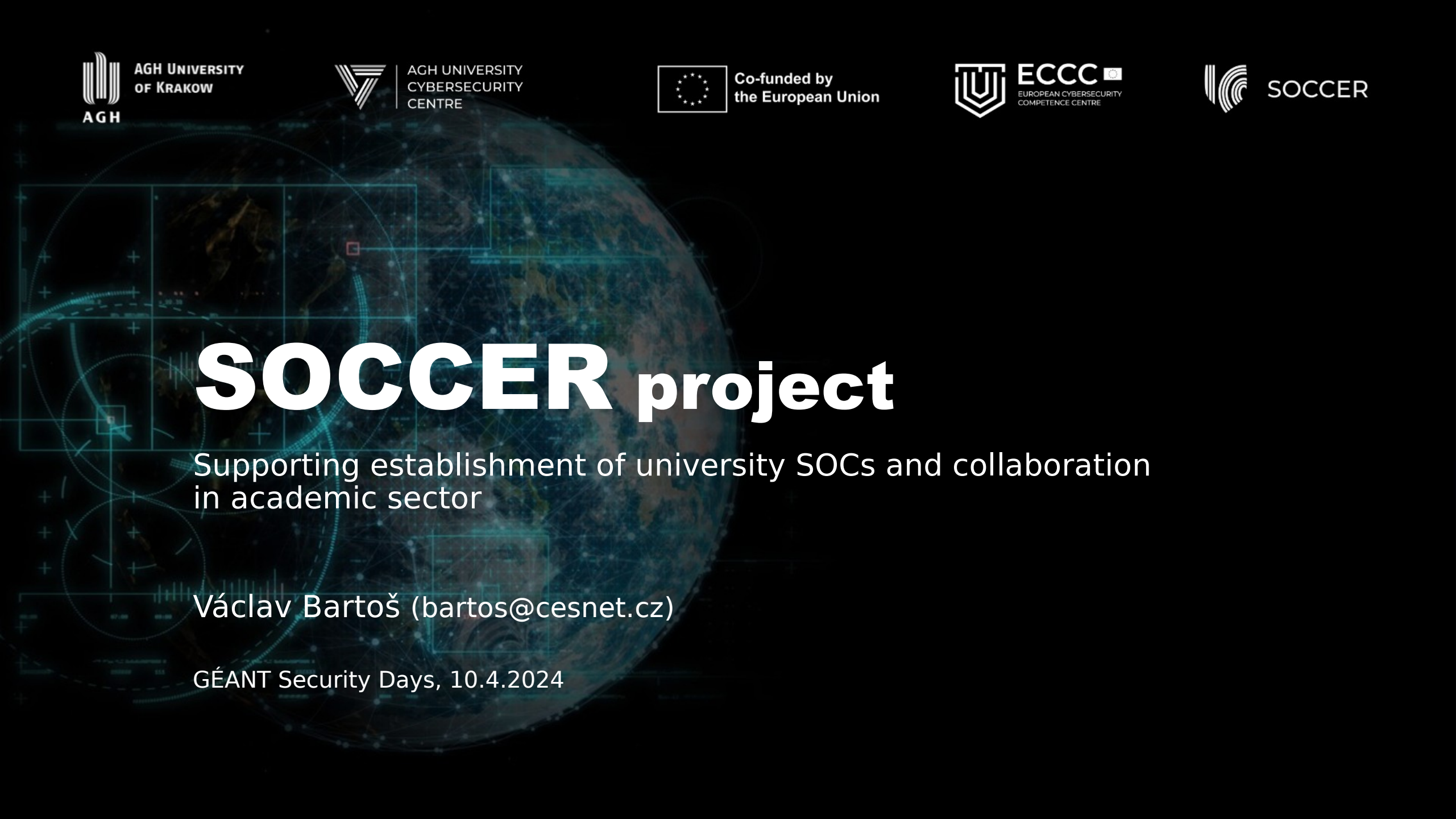


SOCCER project

Supporting establishment of university SOCs and collaboration in academic sector

Václav Bartoš (bartos@cesnet.cz)

GÉANT Security Days, 10.4.2024

AGH University of Krakow

AGH UNIVERSITY CYBERSECURITY CENTRE

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

SOCCER

SOCCER project info

- 9 universities (from PL, CZ, SK, LT, EE) + CESNET (CZ)
- Started 10/2023
- Main goals:
  - Support creation of SOCs at participating universities
  - Create **SOC4Academia toolbox**
  - Establish a **CTI sharing ecosystem** for academia

AGH University of Krakow

AGH University Cybersecurity Centre

Co-funded by the European Union

ECCC European Cybersecurity Competence Centre

SOCCER

SOC4Academia toolbox

- A set of documents aimed to help organizations to build a SOC
- Focused spcifically on academic organizations

- Not reinventing the wheel – based on current best-practices, existing standards, and community materials

Contents:

- SOC models for academia
- Maturity models for SOCs
- SOC organizational and enviromnental requirements for academia
- SOC technical architectures
- Digital Forensics and Incident Response guide
- Software/hardware solution review

AGH University of Krakow

AGH UNIVERSITY CYBERSECURITY CENTRE

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

SOCCER

CTI sharing ecosystem

- Goal – establish an European academic community for sharing CTI
- Not reinventing the wheel or (n+1)th solution
  - Utilization of existing tools
  - Focus on procedures, data and sharing … and **building the community**!
- Just in the beginning … a lot has to be defined
  - What to share (IoCs, vulnerability info, info about incidents, …)
  - How to share (platform(s) / communication channel(s))
  - Rules for CTI exchange

AGH University of Krakow

AGH UNIVERSITY CYBERSECURITY CENTRE

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

SOCCER

CTI sharing ecosystem

- CTI exchange platform (MISP, Warden, ...?)
- Sharing of higher-level cybersecurity information (mailing list?)

- Open to collaboration with existing (or planned) systems/communities

- We need your ideas, proposals, requirements ...

AGH University of Krakow

AGH UNIVERSITY CYBERSECURITY CENTRE

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

SOCCER

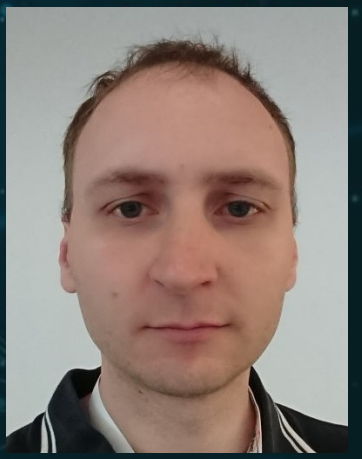
Thank You

Interested in the SOC4Academia toolbox?

Want to joining the CTI sharing community?

Any questions or feedback?

Find me today evening or tomorrow to discuss ...



Václav Bartoš
CESNET
bartos@cesnet.cz

https://soccer.agh.edu.pl/

subscribe to project newsletter there