



# Welcome and Introduction to SCT 2023

**Gerard Frankowski – PSNC ICT Security Department**  
WP9T2

Secure Coding Training 2023 – Poznań, PSNC  
25-27.10.2023

Restricted

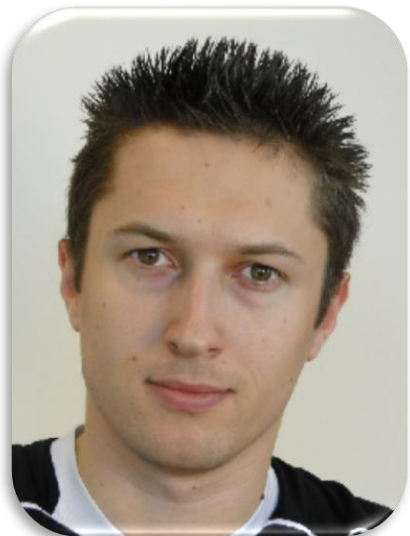
# Agenda

- Hello from the trainers and participants
- **Who and why do SCTs?**
  - PSNC experience on cybersecurity and secure coding
  - Why we are doing the SCTs?
- SCT goes back as F2F!
  - Main organizational issues
- The contents
  - New and updated topics since SCT 2022
  - SCT 2022 Agenda – days 1-3
- Useful details
  - Exercises and activities in breakout rooms
  - Coloring conventions and code snippets
  - Wisdom slides
  - Important links

## SCT 2023 Trainers

### **Paweł Berus (PB)**

In PSNC since 2010 – former developer, pentester and security code reviewer



### **Karolina Buchnat (KB)**

Our new colleague, combining cybersecurity passion with Python development competencies



### **Mikołaj Dobski (MD)**

In PSNC since 2010 – developer, CI/CD and ML expert, security analyst



### **Gerard Frankowski (GF)**

In PSNC since 2003 – analyst, security code reviewer, former developer



### **Jarek Wiczorek (JW)**

In PSNC since 2017 – cybersecurity analyst, code reviewer and Python developer





## SCT 2023 supporting squad and the GLAD Team



**Marcin Wolski (MW)**  
WP9T2 Task Leader  
prepared the  
presentation of  
services offered by  
our task



**Maciej Łabędzki (MŁ)**  
– will tell you about  
School for Software  
Engineering – **TBC**



**Lisa Melrose**



**Dom Mayerl**



**Many thanks to the  
GLAD team!**

Time for our Attendees!

HELLO





## Cybersecurity in

- **P**oznań **S**upercomputing and **N**etworking **C**enter
- Polish NREN (**PIONIER**) operator
- Polish Optical Internet Research Center (**CBPIO**)
  - Over 20 laboratories, e.g. Laboratory of Cybersecurity and Critical Infrastructures Protection
- **PSNC Cybersecurity Department: 29** colleagues as for now
- **ISO 27001** certified (ISMS)
- **ISO 9001** certified, concerning e.g. ICT consulting and cybersecurity audits
- **CyberSec:** Part of EDIH (**European Digital Innovation Hub**) network, including source code security services
  - More: <https://cyber-sec.net.pl>

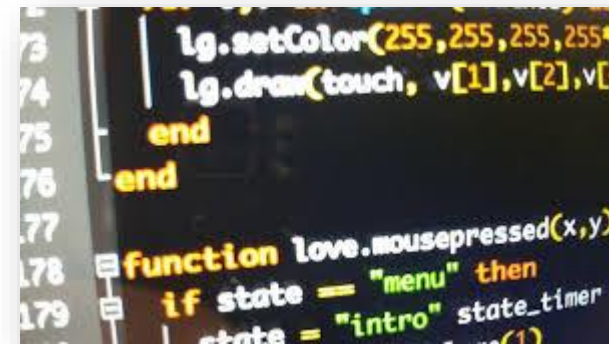


**EDIH**  
European  
Digital Innovation  
Hubs Network



## PSNC experience on source code security

- Secure Coding Trainings
  - GÉANT: 12x (2010-2022) + 1 repetition (2018)
  - National Data Storage (2011-2012)
  - SECOR (2013)
  - E-textbooks: 3x (2013-2014)
  - SCADvance (2017)
  - Single presentations on different events, e.g. EGEE' 09, SECUREX international fair
- Code security reviews
  - Projects: EGEE-II, EGEE-III, GN3, GN3+, GN4/GN4-2/GN4-3, PL-Grid, PL-Grid+, PL-Grid NG, NDS, e-Textbooks, SCADvance, EDWIN, MEDICS
  - Others: e-banking services, Web applications, dLibra, internal reviews
  - Languages: mainly Java, C/C++/C#, PHP, Python





## Why we are doing SCTs?

- The main purposes of the SCT trainings:
  - To **keep the awareness**
  - To **practice** good templates
  - To **explain particular issues** useful for secure development of GÉANT services
- Through this SCT, we want you to:
  - Become familiar with **security requirements** for development of Web applications in several areas
  - Experience the nature of certain types of Web applications **security vulnerabilities**





## SCT on the road again!

- First time F2F since 2019!
- People got accustomed to VCs but F2F workshops are more effective
  - ...And how to organize social events via Zoom?

- Thus after...
  - Poznań
  - Prague
  - Berlin
  - Utrecht
  - Lisbon

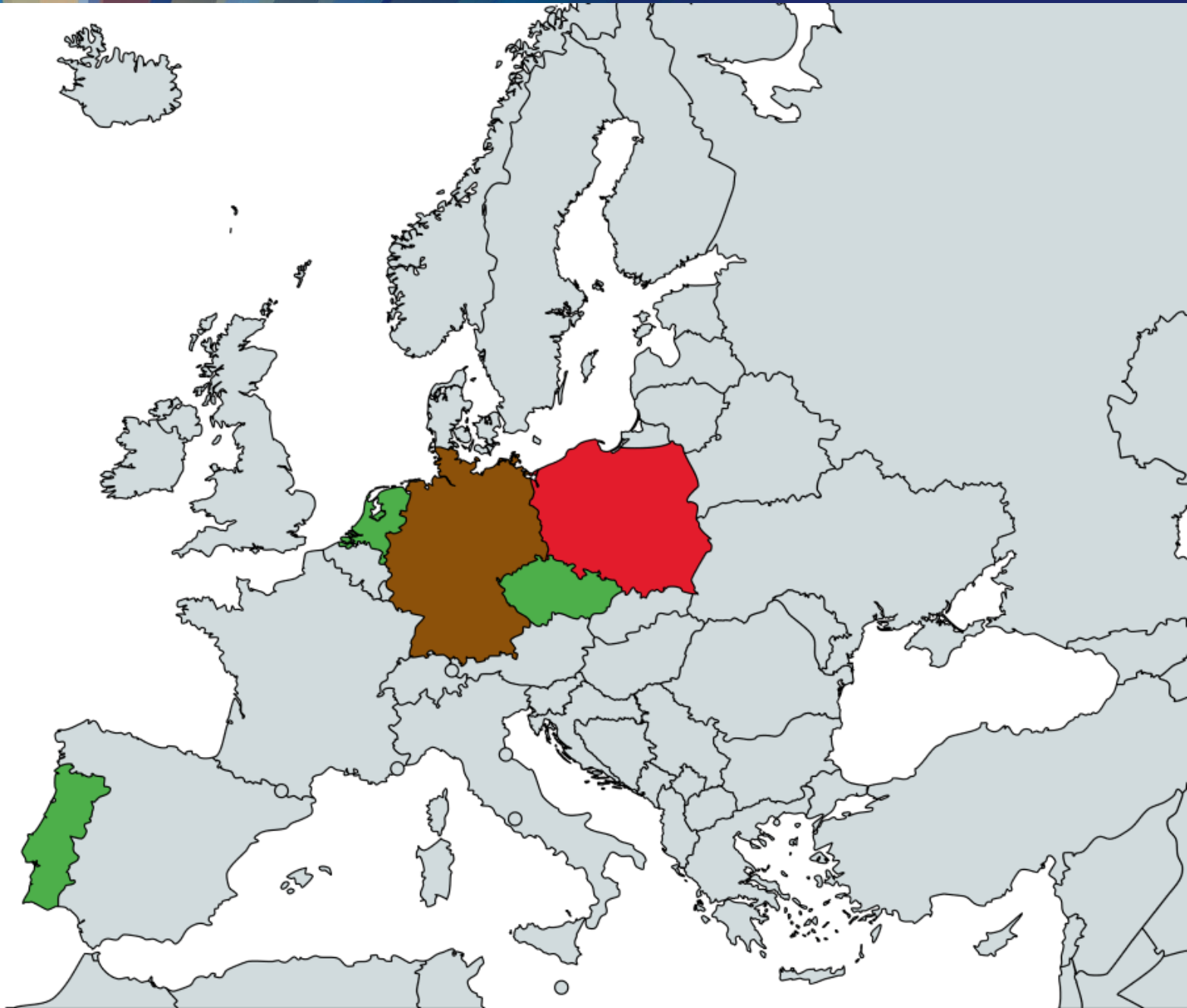


- ...we have invited you to Poznań again!



SCT 2010-2019

- 1 SCT
- 2 SCTs
- 4 SCTs



## SCT 2023 – main organizational issues

- We return to the usual F2F SCT schedule
- 3 days
  - Day 1: afternoon (13:00-17:00 CEST)
    - More high level issues + ASVS
  - Day 2: the whole day (9:00-17:00 CEST)
    - Python secure programming day!
  - Day 3: morning (9:00-13:00 CEST)
    - A bit of ASVS + HackMe
- Two main workshops finalize Days 2 and 3
  - Day 2 – Python secure programming workshop
  - Day 3 – HackMe contest
- Social event – Day 2
- Feedback collection – Day 3





## New and updated topics since SCT 2022

- Added:
  - **Python secure programming**
  - OWASP ASVS
    - V3 – Session Management
    - V12 – Files and Resources
  - Technical dinner 😊
- Updated or adjusted:
  - HackMe contest
  - CI/CD and SDLC issues



# Topics

## SCT 2023 Agenda – day 1 (Wednesday, 25th October)

Time	Topic	Who
13:00-13:40	Welcome and introduction to SCT 2023	GF
13:40-13:55	WP9T2 - Software Governance for the GÉANT community	MW
13:55-14:00	Invitation to School of Software Engineering 2024	MŁ
14:15-15:45	<b>Continuous Integration / Continuous Development and Secure Development Life Cycle</b>	MD
16:00-17:00	<b>Writing Hacker Proof Code - Files and Resources</b>	GF

Breaks not shown



## SCT 2023 Agenda – day 2 (Thursday, 26th October)

Time	Topic	Who
9:00-9:50	Secure Programming in Python – Introduction	KB, JW
9:50-11:00	Secure Programming in Python – Python gotchas (1)	KB, JW
11:15-12:00	Secure Programming in Python – Python gotchas (2)	KB, JW
12:00-13:00	Secure Programming in Python – secure coding practices (1)	KB, JW
13:45-15:00	Secure Programming in Python – secure coding practices (2)	KB, JW
14:20-15:00	Secure Programming in Python – tools and conclusions	KB, JW
15:15-17:00	Secure Programming in Python – practical workshop	KB, JW

Breaks not shown





## SCT 2023 Agenda – day 3 (Friday, 27th October)

Time	Topic	Who
9:00-10:20	<b>Writing Hacker Proof Code - Session Management</b>	GF
10:30-10:50	HackMe – Preparations and Instructions	PB
11:00-12:30	<b>HackMe contest</b>	PB
12:40-12:50	HackMe Evaluation and Solutions	PB
12:50-13:00	SCT 2023 Summary and Closing	GF

Breaks not shown



## In-place exercises

- You will be shown an exercise (sometimes plus the expected time to provide a solution)
- You will be asked to present your solutions and we will be discussing them
  - Our exemplary solutions do not have to be neither the only nor the best ones
- The presentations will contain solution slides, possibly with additional comments
- Later you will be provided full PDF slides



# Coloring of code snippets and good / bad patterns

## Convention 1 (the old one)

This is the background to present a bad coding (configuration) pattern

And this is to present a proper template or pattern

This is neutral, just to show some example

And this is the way we denote **an important part** of the source code in a larger listing



## Coloring of code snippets and good / bad patterns

### Convention 2 (Python Secure Programming part)

Code fragments containing errors or other problems have been marked with a pink dashed box.

Neutral code fragment, i.e. not marked (as good or bad).

Code fragments that are correct and do not contain errors are marked with a green box.

```
variable1 = 10  
variable2 = "Hello"  
variable3 = [1, 2, 3]  
# code coloring follows the IDE editor
```



## The content of code snippets

- Remember that even the recommended code patterns may not be the full solution!
  - They present a particular isolated issue and then address it
  - But the real, full pattern could exceed one or several slides...
- **So do not copy this code directly into your project, just use the provided good patterns**





**You will find words of wisdom on similar slides.  
Remember them!**





**You will find words of wisdom on similar slides.  
Remember them!**



## Other SCT 2023 tips

- Please ask questions at once!
- Tell us when you need an extra break
  - The agenda is subject to change when the actual pace needs it
  - But we will finish on time





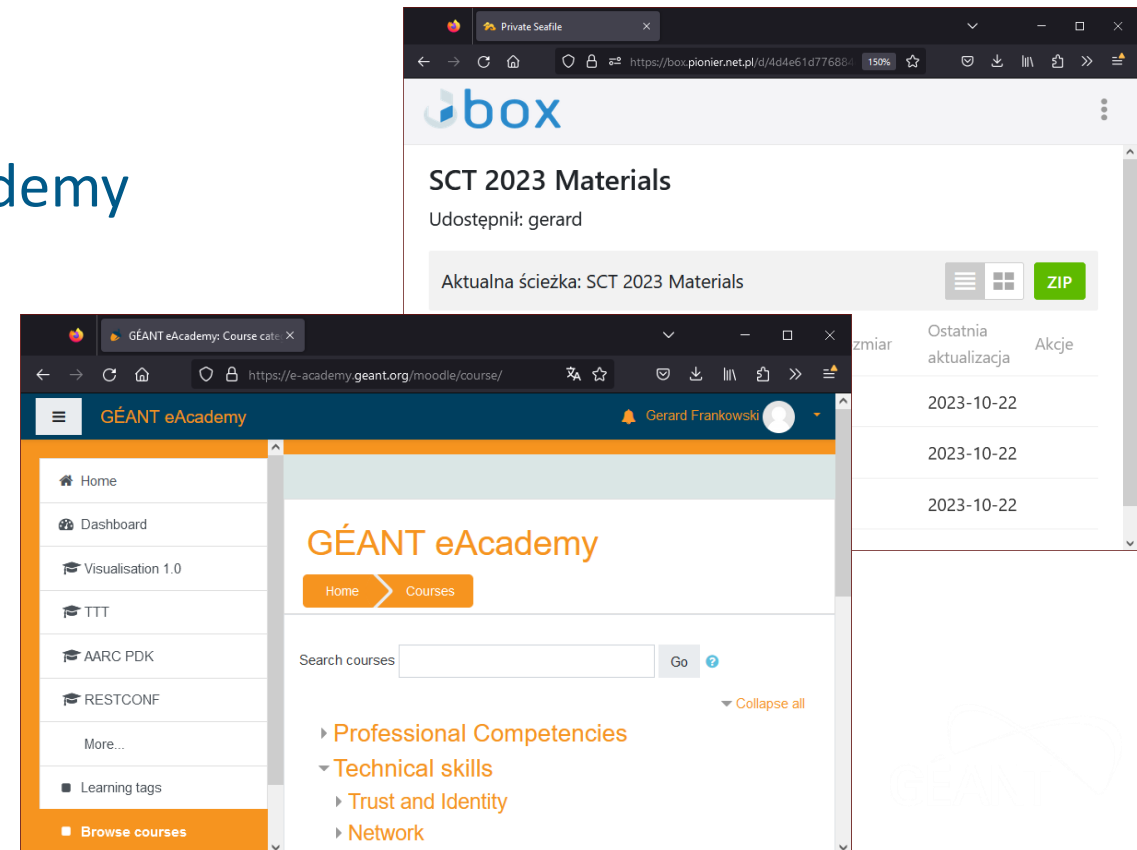
## Your feedback is crucial!

- This year we will have a printed-out evaluation form
  - Our experience says this is the most effective form of feedback collection :)
- Evaluation form is **anonymous**
- We suggest to fill the form during the timeframe for HackMe contest results evaluation
  - Friday between 12:40-12:50
  - Should take no more than 5 minutes
- You may also suggest your favorite topics for future SCTs!



## Presentations and recordings

- **Links** for content to download or access after SCT 2023
  - PSNC cloud shared folder for presentations, recordings, etc.
    - <https://box.pionier.net.pl/d/4d4e61d776884e03bf1a/>, or
    - <https://tinyurl.com/SCT23-repo>
- We also will upload SCTs contents to eAcademy
  - <https://e-academy.geant.org/moodle/>





# Thank You

Any questions?

[gerard@man.poznan.pl](mailto:gerard@man.poznan.pl)

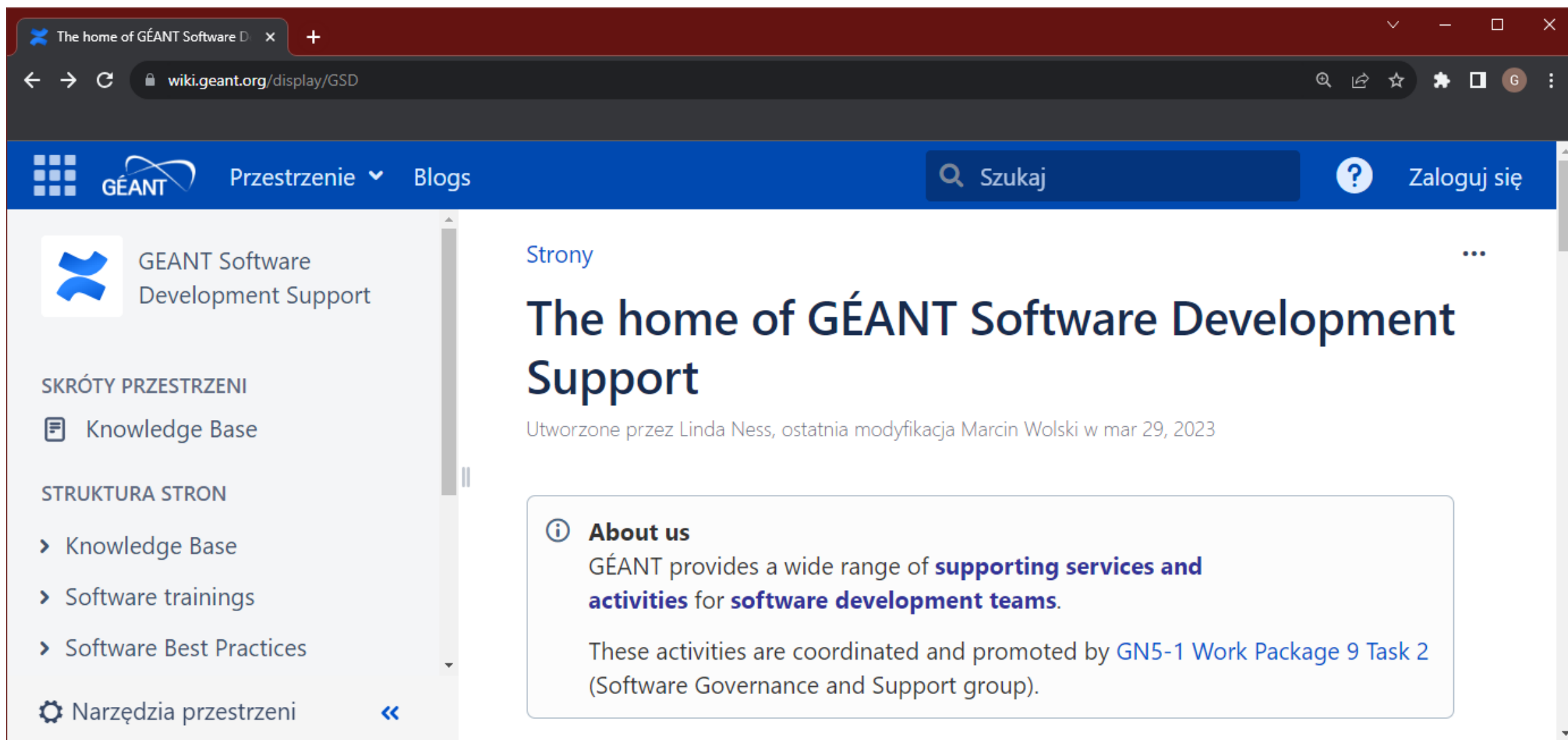
[www.geant.org](http://www.geant.org)



Co-funded by  
the European Union

The project co-financed by Polish Ministry of Science and Higher Education from financial resources of the programme entitled "PMW"

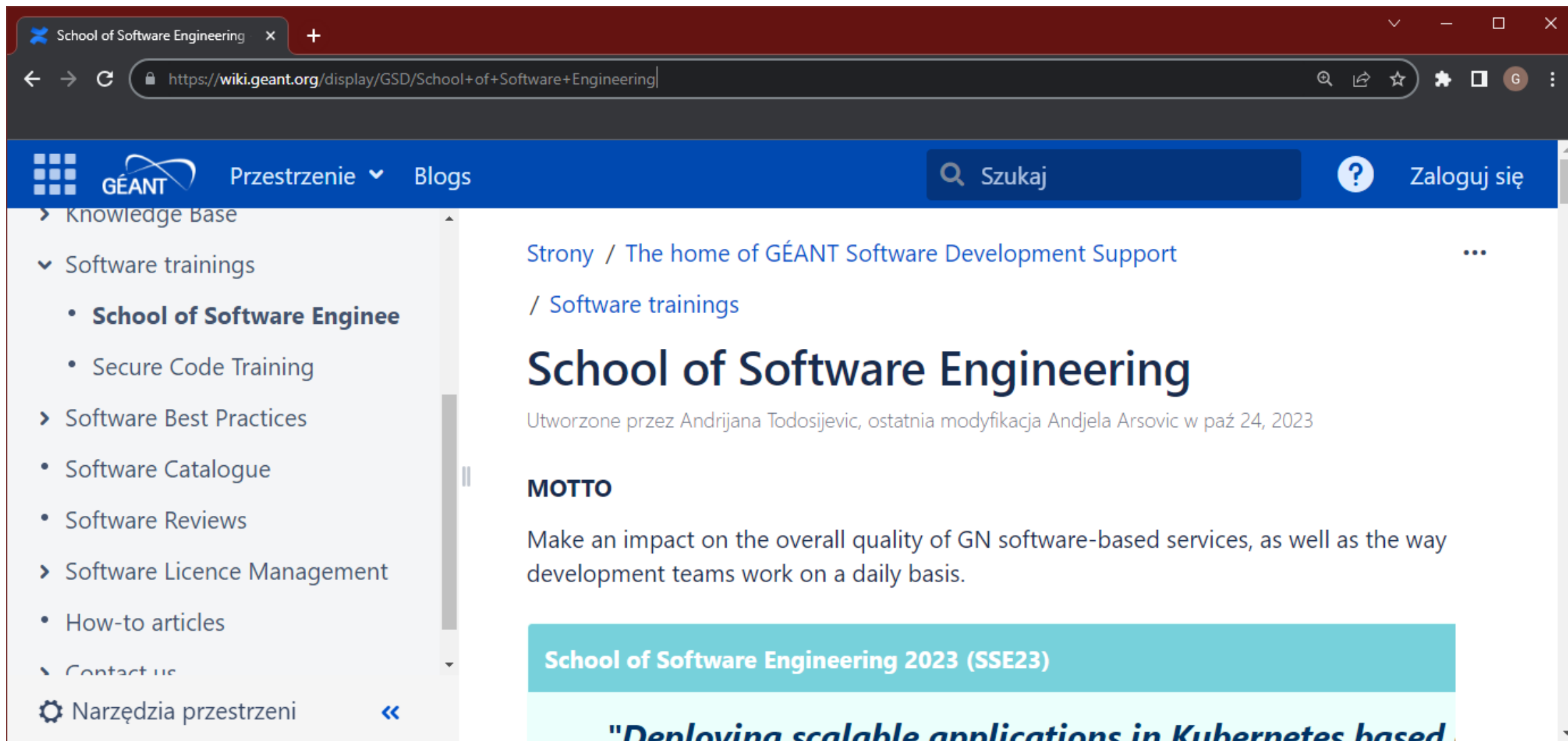
## GN5-1 WP9T2 Landing Page - <https://wiki.geant.org/display/GSD>



The screenshot shows a web browser window displaying the GEANT Wiki page for GSD. The browser's address bar shows the URL [wiki.geant.org/display/GSD](https://wiki.geant.org/display/GSD). The page header features the GEANT logo, navigation links for 'Przestrzenie' and 'Blogs', a search bar with the text 'Szukaj', and a 'Zaloguj się' button. The main content area is titled 'Strony' and 'The home of GÉANT Software Development Support', created by Linda Ness and last modified by Marcin Wolski on March 29, 2023. A sidebar on the left provides navigation options under 'SKRÓTY PRZESTRZENI' (Knowledge Base) and 'STRUKTURA STRON' (Knowledge Base, Software trainings, Software Best Practices), along with 'Narzędzia przestrzeni'. The main content includes an 'About us' section with the following text:

**About us**  
GÉANT provides a wide range of **supporting services and activities** for **software development teams**.  
These activities are coordinated and promoted by [GN5-1 Work Package 9 Task 2](#) (Software Governance and Support group).

# School of Software Engineering Landing Page - <https://wiki.geant.org/display/GSD/School+of+Software+Engineering>



The screenshot shows a web browser window displaying the landing page for the School of Software Engineering on the GEANT wiki. The browser's address bar shows the URL: <https://wiki.geant.org/display/GSD/School+of+Software+Engineering>. The page features a blue header with the GEANT logo, navigation links for "Przestrzenie" and "Blogs", a search bar labeled "Szukaj", and a "Zaloguj się" button. A left sidebar contains a menu with categories like "Knowledge Base", "Software trainings", "Software Best Practices", and "Software Licence Management". The main content area displays the breadcrumb "Strony / The home of GÉANT Software Development Support / Software trainings", followed by the title "School of Software Engineering" and its creation/modification details. A "MOTTO" section contains the text: "Make an impact on the overall quality of GN software-based services, as well as the way development teams work on a daily basis." At the bottom, a teal banner highlights "School of Software Engineering 2023 (SSE23)" with a quote: "Deploying scalable applications in Kubernetes based".

School of Software Engineering

Strony / The home of GÉANT Software Development Support / Software trainings

Utworzone przez Andrijana Todosijevic, ostatnia modyfikacja Andjela Arsovic w paź 24, 2023

**MOTTO**

Make an impact on the overall quality of GN software-based services, as well as the way development teams work on a daily basis.

School of Software Engineering 2023 (SSE23)

"Deploying scalable applications in Kubernetes based