



Cyber  
Security  
Vlaanderen

# Cybersecurity Research Program Flanders



# Cybersecurity Research Program Flanders

A brief overview of the research program

Insight into its core activities

An overview of its impact on industry and the broader ecosystem

Tine Verhanneman

Research Manager  
Cybersecurity

KU Leuven

# Cybersecurity Research Program Flanders



- ✓ A flagship initiative under the Flanders Policy Plan Cybersecurity by the Flemish Government
- ✓ Launched in 2019 with a 10-year horizon (until 2028)
- ✓ Cybersecurity Research Consortium Flanders



# Flanders Policy Plan Cybersecurity



## Cybersecurity *Research Program*

Strengthening top cybersecurity research in Flanders



## CS implementation in companies

Enhancing the cybersecurity maturity of companies and promoting the adoption of innovative cybersecurity solutions.



## Flanking policy

Promoting broad awareness and delivering training in cybersecurity



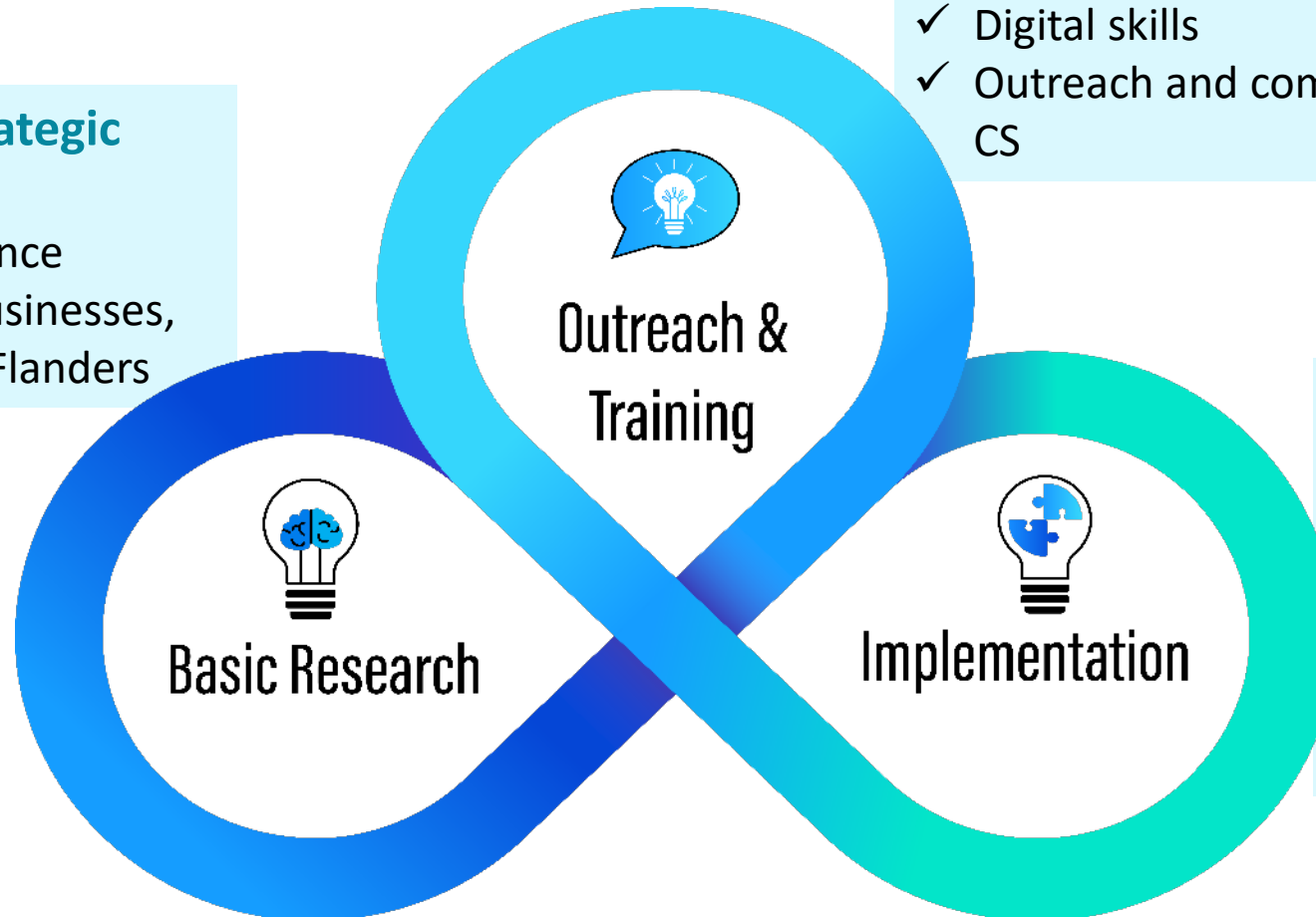
# Research Program within the Flanders Policy Plan

## CORE mission: Strategic Basic Research

- ✓ Academic excellence
- ✓ Synergies with businesses, companies, ... in Flanders

## Flanking Policy

- ✓ PhD schools
- ✓ Employee trainings
- ✓ Digital skills
- ✓ Outreach and communication on CS



## Increase CS-maturity in companies

- ✓ Support companies in increasing awareness and maturity
- ✓ Inform and advise companies on the application of innovative CS solutions

# Research Consortium

**KU LEUVEN** **DistriNet**

**KU LEUVEN**



COSIC

**KU LEUVEN** **CiTiP**



SOFTWARE  
LANGUAGES  
LAB



RDI



Computing Systems Lab

**imec**

## Program Directors



Prof Wouter Joosen  
DistriNet KU Leuven



Prof Bart Preneel  
COSIC KU Leuven

## 7 research groups

### Approx 250 affiliated researchers

- 50 faculty & permanent research staff
- 200+ researchers: PhD & PostDoc

# Research Tracks and Objectives

**TRACK  
01**

**SECURE  
SOFTWARE  
&  
APPLICATIONS**

**TRACK  
02**

**SECURITY  
SERVICES &  
SECURE  
PLATFORMS**

**TRACK  
03**

**SYSTEM &  
INFRA-  
STRUCTURE  
SECURITY**

**TRACK  
04**

**SECURE  
HARDWARE  
& BUILDING  
BLOCKS**

## Strategic objectives:

- “Defensive” research
- Strengthening inter-federal and European collaboration
- Boost research valorisation by means of prototypes

# CS Research Program: Themes

## TRACK 01

- Secure Software Development Lifecycle
- Program Verification and Cybersecurity Testing
- Secure Programming Languages

**SECURE  
SOFTWARE  
&  
APPLICATIONS**

## TRACK 02

- Security Services
- Cybersecurity of Innovative platforms: DLT, AI and IoT
- Policy and Regulations (GDPR, NIS2, CRA, AI Act, ...)

**SECURITY  
SERVICES &  
SECURE  
PLATFORMS**

## TRACK 03

- System Security
- Network security
- Security Monitoring & Management

**SYSTEM &  
INFRA-  
STRUCTURE  
SECURITY**

## TRACK 04

- Hardware security
- Cryptographic Algorithms (incl. PQC)
- Cryptographic Protocols
- Secure and efficient cryptographic implementations

**SECURE  
HARDWARE  
& BUILDING  
BLOCKS**

# From vulnerabilities to standards: impact of network security research

Network security vulnerabilities have broad real-world impact

- Research repeatedly identified critical Wi-Fi vulnerabilities
  - → Led to improvement in protocols and implementations
  - 2 defenses are standardized and are mandatory in Wi-Fi 7

Combines both offensive and defense research



- Find vulnerabilities & disclose them before they are abused
- Builds expertise to design & evaluate new defenses

From research to  
impact

network security

# From vulnerabilities to global mitigation

## Research on Internet security & Denial-of-Service (DoS) attacks (2024)

- 4+ million vulnerable Internet servers identified
- → vulnerable to Denial-of-Service (DoS) attacks
- Root cause:
  - Use of old protocols
  - misconfigurations
- Coordinated disclosure (CCB, ISPs, ...)
- Collaboration with the Shadowserver Foundation (nonprofit, UK) for monitoring & notification.

From research to  
impact

network security

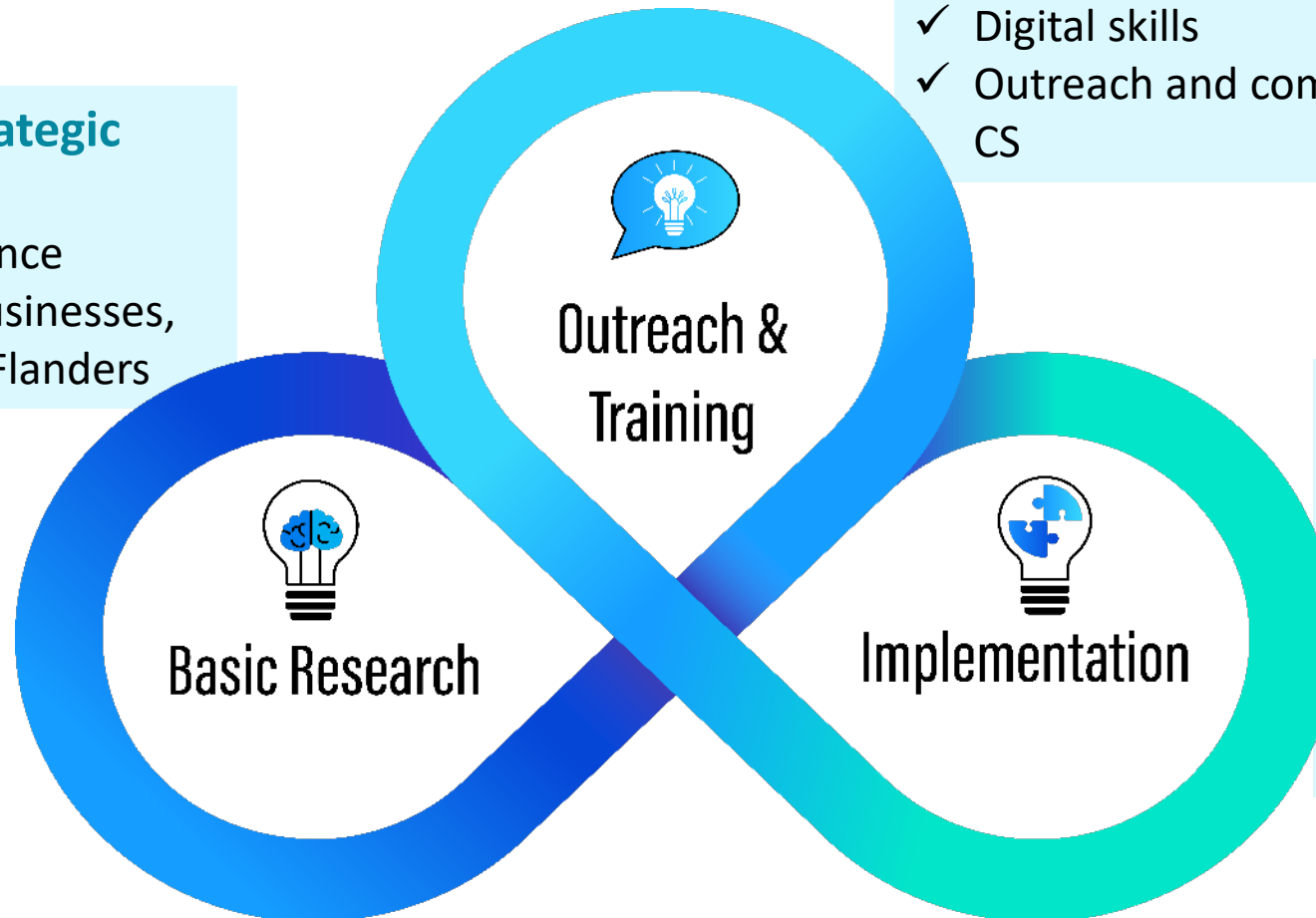
# Research Program within the Flanders Policy Plan

## CORE mission: Strategic Basic Research

- ✓ Academic excellence
- ✓ Synergies with businesses, companies, ... in Flanders

## Flanking Policy

- ✓ PhD schools
- ✓ Employee trainings
- ✓ Digital skills
- ✓ Outreach and communication on CS



## Increase CS-maturity in companies

- ✓ Support companies in increasing awareness and maturity
- ✓ Inform and advise companies on the application of innovative CS solutions

# A growing pipeline of applied research projects (sample)

## Some Themes 2025 (continued '26)

- Security Testing
- Threat Modelling best practices, Security by Design
- Securing AI
- Agentic AI in Security
- Data protection and anonymization

## Themes 2026

- Biometrics and MFA
- PQ roadmaps and agile crypto
- Synthetic data for SOCs, innovation in SOCs
- AI enhanced security operations



TETRA  
COOCK+  
ICON

### Partnerships:

- Educational institutions
- Research Organizations
- Industry associations

# Initiatives focused on Critical Infrastructure

## Cybersecurity in **Critical Infrastructure**:

- Healthcare: collaboration with Shield ( a cybersecurity initiative for hospitals)
- Internet Infrastructure:
  - Analysis of phishing/scam ecosystem based on CCB data of SafeOnWeb
  - Collaborations with DNS registry EURid
- Finance: collaborations with regional Financial Institutes

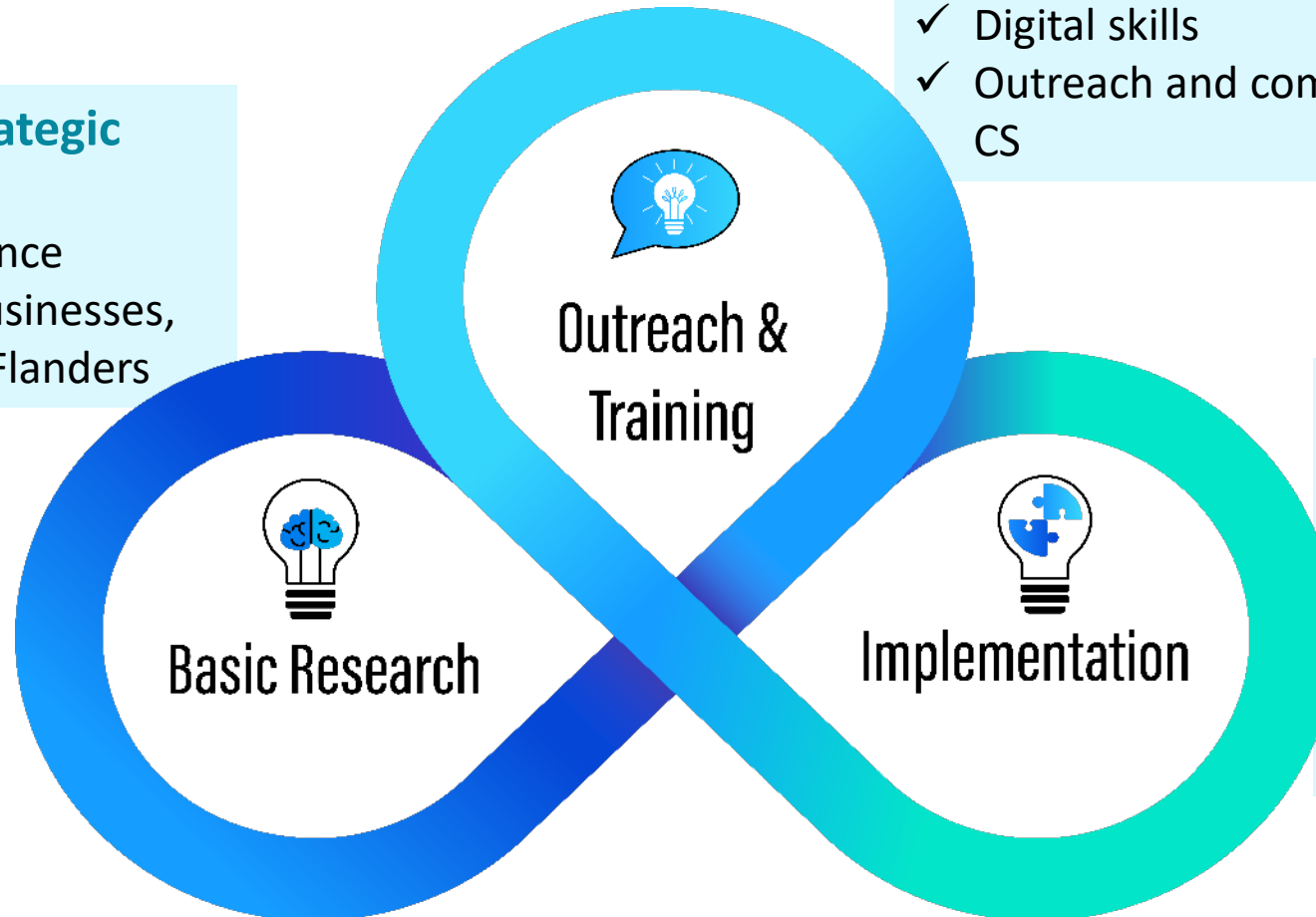
# Research Program within the Flanders Policy Plan

## CORE mission: Strategic Basic Research

- ✓ Academic excellence
- ✓ Synergies with businesses, companies, ... in Flanders

## Flanking Policy

- ✓ PhD schools
- ✓ Employee trainings
- ✓ Digital skills
- ✓ Outreach and communication on CS



## Increase CS-maturity in companies

- ✓ Support companies in increasing awareness and maturity
- ✓ Inform and advise companies on the application of innovative CS solutions

# Contribution to high-impact industry training and expert gatherings

- Flanking policy
- Summer schools
- Course materials



Leuven, Faculty Club

### AI Red Teaming 2-day workshop

Gary Lopez, TinyCode

February 19-20, 2026

KU LEUVEN Cyber Security Flanders



### Workshop on Hacking LLM Guardrails

November 26, Leuven

KU LEUVEN VLAIO sirris Cyber Security Flanders



SEPT. 11, 13:30-18:00 - KU LEUVEN, AULA DUVAL

### CYBERSECURITY WITH AI AND FOR AI: A REAL-WORLD INDUSTRY PERSPECTIVE

Cyber Security Flanders KU LEUVEN



ACADEMIC INSIGHTS,  
INDUSTRIAL IMPACT:

### THE FUTURE OF IOT SECURITY TESTING

MAY 15, GHENT

KU LEUVEN VUB VLAIO Cyber Security Flanders

# Contribution to high-impact industry training and expert gatherings

- Flanking Policy
- Summer schools
- Course materials



# Contribution to high-impact industry training and expert gatherings

- Flanking Policy
- Summer schools
- **Course materials**



# Outreach to a broad audience



- Knowledge transfer (blog posts, white papers, ...)
- Training
- Newsletter
- Events



# Cybersecurity Bites



**VIBE CODING**  
Beveiligingsrisico's  
bij AI-gedreven  
softwareontwikkeling

**KOMPAS**  
WEGWIJS IN CYBERSECURITY



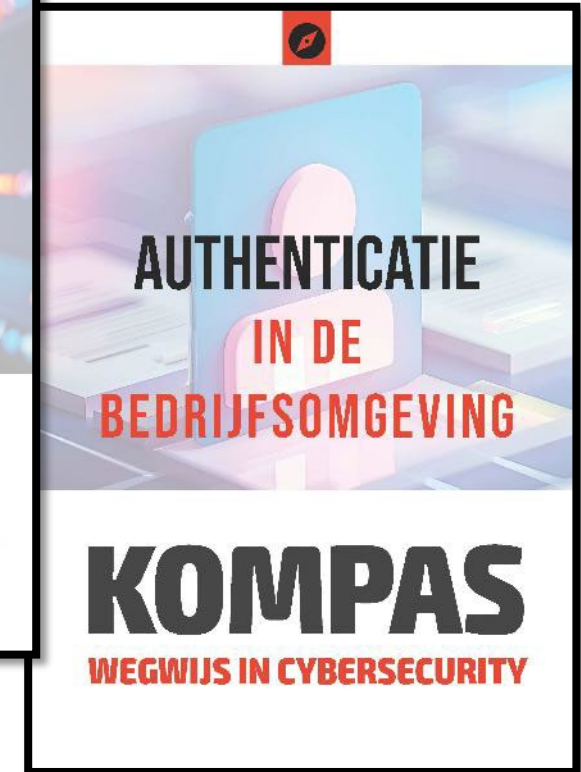
**CYBERDREIGINGS-  
LANDSCHAP**  
EEN BLIK OP 2026

**KOMPAS**  
WEGWIJS IN CYBERSECURITY



**HOE JE WEBAPP  
VEILIG IN PRODUCTIE  
BRENGEN?**

**KOMPAS**  
WEGWIJS IN CYBERSECURITY



**AUTHENTICATIE  
IN DE  
BEDRIJFSOMGEVING**

**KOMPAS**  
WEGWIJS IN CYBERSECURITY

# Cybersecurity Bites



nieuwe technologieën

blocked

### DE IMPACT VAN AI OP DE WERELDWIJDE INTERNETCENSUURCRISIS

Artificiële Intelligentie (AI) wordt vaak tweemaal...



cyberwijs voor kmo's

### SOAR IS DOOD. LANGE LEVE SOAR.

Een effectief incidentresponsplan vormt een belangrijk onderdeel...



Cyber Security  
Vlaanderen

## nieuwsbrief

november 2024

IN DEZE NIEUWSBRIEF  
Industry Day | Valorisatie |  
Onderzoek | Implementatie |  
Kalender

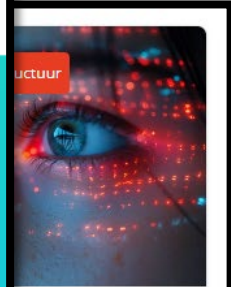
### CYBERSECURITY INDUSTRY DAY: 14 NOVEMBER

**Cybersecurityonderzoek met Impact**

Op 14 november slaan we de brug tussen cybersecurityonderzoekers en innovatoren uit overheid en bedrijfswereld. Op de agenda: keynotes, breakouts, demo's en netwerking. Deze namiddag staat open voor onderzoekers, tech-ondernemers, innovatoren en beleidsmakers met interesse in cybersecurity. De editie 2024 brengt **20+ live demo's**, waaronder concrete resultaten uit samenwerking met de industrie.



STRUCTUUR



EN VAN RNING VOOR EID

kan een

kompas: cybersecurity bijdragen met industrieel perspectief

### HET BELANG VAN SECURITY BY DESIGN BIJ DE ONTWIKKELING VAN SOFTWARE

Wat verstaan we onder security by design bij de ontwikkeling van veilige en betrouwbare software?

LEZEN

### CYBERDREIGINGSLANDSCHAP EEN BLIK OP 2024

Welke verschuivingen in cyberaanvals- en verdedigingsstrategieën brengt 2024, en wat is de rol van Artificiële Intelligentie hierin?

LEZEN

### NAVIGEREN DOOR DE JURIDISCHE ASPECTEN VAN ARTIFICIËLE INTELLIGENTIE EN CYBERVEILIGHEID

Wat is de impact van AI-systemen op de cyberveiligheid en hoe reageert de Europese wetgeving hierop?

LEZEN

adverteerders steeds slimmere manieren vinden om gebruikers te volgen, werken browsers en regelgeving aan tools om jouw privacy te beschermen. Dit artikel neemt je mee in de evolutie van online tracking in...

LEZEN

3 JAN 2025 | 4 MINUTEN

Belangrijke rollen spelen in cybersecurity, maar de implementatie ervan blijkt complex. Wat zijn de obstakels? En op welke manier kan een gerichte aanpak machine learning toch effectief maken? 2010 kende een opvallende trend: machine learning...

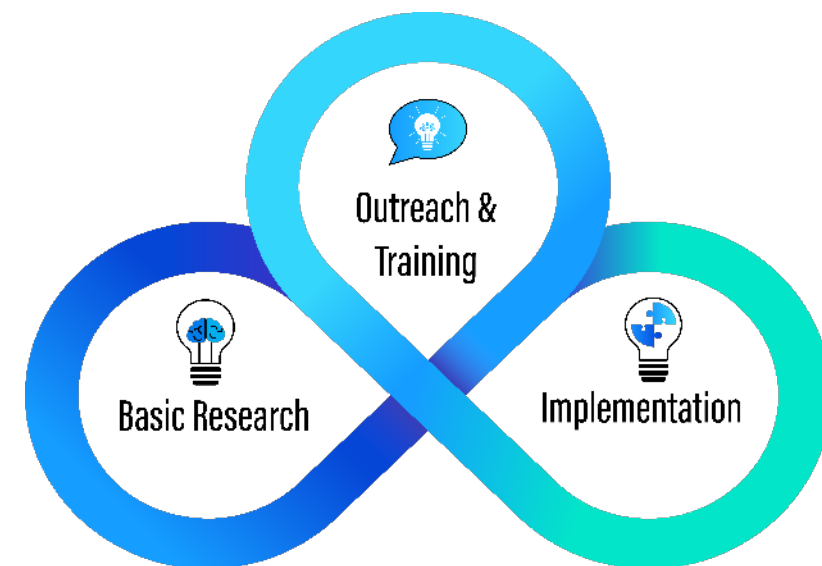
LEZEN

30 DEC 2024 | 6 MINUTEN

# Conclusion

- Cybersecurity remains a growing and evolving challenge
- The program combines cutting-edge research with real-world impact
- From research to impact:
  - Innovative solutions and mechanisms
  - Technology transfer, training, and outreach
  - Strong collaboration with industry and stakeholders
- The program contributes to a stronger cybersecurity ecosystem

*Key take away: sustained collaboration is essential to drive adoption and impact.*





Cyber  
Security  
Vlaanderen

# Thank You

 [cybersecurity-research.be](https://cybersecurity-research.be)

 [cybersecurity-bites.be](https://cybersecurity-bites.be)

 [tine.verhanneman@kuleuven.be](mailto:tine.verhanneman@kuleuven.be)

