KU LEUVEN

Cyber resilience
series 2025

From 11 February until 18 November 2025
KU Leuven, Campus Rabot (8 sessions)

PUC | CONTINUE

Scope and overview

In an increasingly technology-driven world, cybersecurity stands as the cornerstone of digital resilience. In this programme, we will explore the full spectrum of cyber resilience, from prevention to response, while gaining both immediate, hands-on skills and foresight for the future of cybersecurity. This programme brings together academic researchers and industrial experts, and thus provides a blend of lectures and use cases and practical testimonials.

This overview course is structured into eight sessions. We start with an overview of methodologies and technologies, beginning with a holistic view of cybersecurity in a digital ecosystem (session 1). Cybersecurity plays a critical role in ensuring data privacy, which involves complying with privacy laws and regulations like GDPR (session 2). The programme then progresses to hands-on workshops: one focused on network security (session 3) and another on the protection of the growing category of embedded ‘IoT’ devices (session 4). As standards and certifications also play an increasing role in implementing cybersecurity measures, this is the focus of the next session (session 5). We learn how (not) to respond, when a cyberattack occurs, and hear the lessons learned from a 'victim' (session 7). Finally, we look ahead to what the future holds, especially in the context of cybersecurity in the era of quantum computing (session 8).

Target audience

This programme is tailored to professionals looking to deepen their (technical) knowledge in various aspects of cyber resilience/a broad range of cybersecurity aspects.

- Prior knowledge required: a minimal basic knowledge of IT is required, without having to be a specialist.
- Participating companies are not required to have the same employee attend all sessions. If you enrol as a company for the whole series, you have the flexibility to send a different employee to each session.

Programme

Session 1: Tackling cybersecurity challenges: a complex security puzzle

11 February 2025 - Vincent Naessens (KU Leuven)

This introductory session provides insight into the complexity of the security puzzle that needs to be solved. A **wide range of building blocks** for developing and maintaining digital applications and infrastructure is presented. Each of these puzzle pieces serves a specific purpose and addresses a portion of the cybersecurity challenges. During the session, it becomes clear that cybersecurity is a concern throughout the entire lifecycle of digital systems. Furthermore, a silver bullet is unfortunately not on the table. We focus on **methodologies and technologies** for the development of secure digital applications.

For this session, no technical prior knowledge/background is needed.

Session 2: ‘Privacy by design': a technical approach to privacy risk

11 March 2025 - Kim Wuyts (PwC)

Since the implementation of the GDPR in 2018, GDPR sets the legal framework for protecting personal data. It requires '**appropriate technical measures**' and privacy by-default and by-design approaches to be implemented. In this session, we'll dive deeper in the world of privacy by design. We tackle **concrete guidelines** on how to incorporate privacy by design in your development process.

This will include:

- Privacy engineering 101 (why, what, how)
- Privacy threat modeling as guide
- Privacy Enhancing Technologies (de-identification techniques, privacy-preserving solutions)
- Integrating privacy in your secure development lifecycle

This session is aimed at IT professionals and developers.

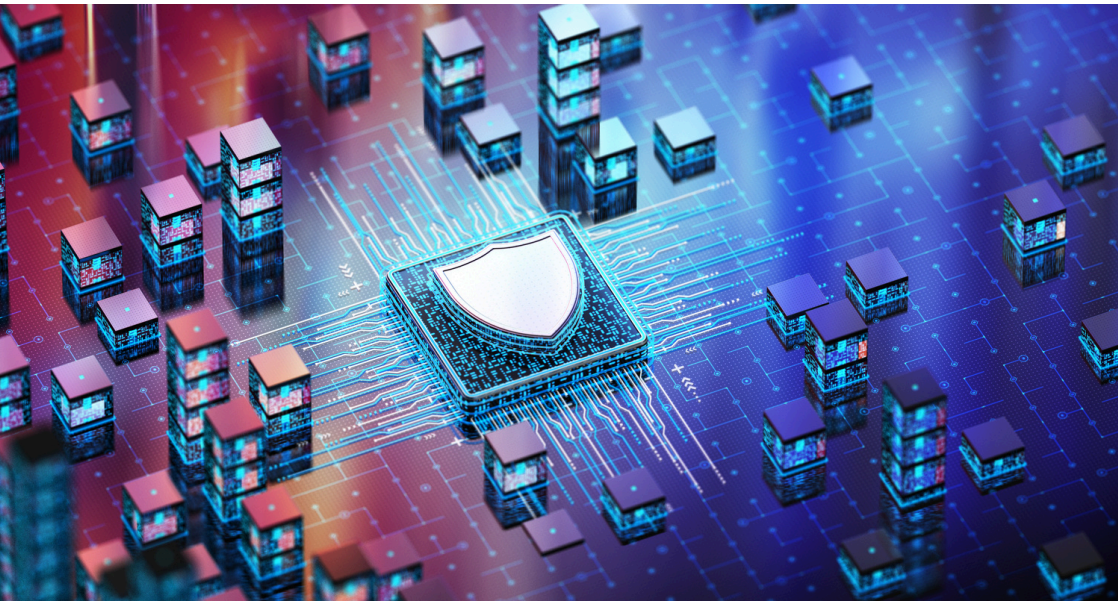
Session 3: Efficient use of a 'network protocol analyzer' in cyber threats (workshop)

22 April 2025 - Tom Cordemans (KU Leuven)

Many companies rely on a Security Information and Event Management system (SIEM) to consolidate data from various applications and equipment, allowing them to maintain an overview of their security landscape. To investigate alerts generated by their SIEM system more thoroughly, they turn to a Network Protocol Analyzer (NPA). An NPA captures, analyzes, and visualizes network traffic and can have a broad range of applications.However, the procedures and configurations of NPAs vary according to the specific issue at hand (cybersecurity, troubleshooting, etc.), which often leads to incorrect or inefficient usage in practice.

During this workshop, we will build the knowledge and skills necessary to use Network Protocol Analyzers correctly and efficiently, particularly in the context of cybersecurity threats. We will work with real-life scenarios and gain practical insights into the underlying workings of NPAs. The NPA that we will delve deeper into during the workshop is the open-source NPA, **Wireshark.**

This workshop is intended for system administrators, network administrators, SOC analysts, security engineers, and individuals in similar roles. A solid background in network protocols and network analysis is a prerequisite (CompTIA Network+, CCNA, etc.).



Session 4: Hacking and protecting embedded devices (workshop)

13 May 2025 - Jorn Lapon (KU Leuven)

The Internet of Things (IoT) presents significant opportunities for businesses, but it also introduces unique and new security challenges. ‘Smart’ devices connected to the internet serve as potential entry points for cybercriminals and can render your company exceptionally vulnerable. Enhanced cybersecurity for embedded devices and systems is therefore essential.

In this workshop, you will gain practical insights into security issues related to embedded systems. We will delve into seven typical **IoT hacks**, providing you with hands-on knowledge of common vulnerabilities in embedded devices, contemporary attacks, and security technologies. Additionally, you will become familiar with security guidelines (OWASP) for designing, developing, and maintaining new embedded systems. By the end of the workshop, you will have the expertise to detect common vulnerabilities and enhance the security of embedded devices.

This workshop is aimed at developers of embedded systems and IoT.

Session 5: EU cybersecurity standards and regulation for IoT ecosystems and Industrial Control Systems

10 June 2025 - Vincent Naessens (KU Leuven)

In this session, we will delve into the critical landscape of cybersecurity standards and regulations within the European Union, specifically tailored for **IoT ecosystems** and **Industrial Control Systems**. The overview encompasses the diverse realm of IoT systems, including smart devices found in retail outlets. Additionally, we address Industrial Control Systems crucial to sectors such as rail and energy, emphasizing the importance of compliance with EU cybersecurity standards to fortify the security posture of these interconnected systems.

This session is aimed at developers, integrators, and operators deploying embedded systems.

Session 6: NIS2 and the broader regulatory framework: update

9 September 2025 - Patrick Banken (Kappa Data), TBC

With the NIS2 directive transposed into national legislation as of October 2024, where do we currently stand? What are the next steps for enhancing cybersecurity regulations across the EU? Beside the broader regulatory framework, we will also discuss in this session the major challenges which IT partners and their customers have faced in recent months during the implementation period, and we'll present a selection of effective tools.

This session is aimed at legal and compliance officers, CISO's, IT and network specialists, as well as C-level executives and general management profiles.

Session 7: Cyberattack response

14 October 2025 - Tom Bauwens (Eubelius), Kalman Tiboldi (TVH)

This session offers a comprehensive guide to responding to cyber-attacks within the law. It covers the **legal considerations** of cyber incidents, including criminal law, data protection, privacy laws, and regulatory compliance.

We start by analyzing **the anatomy of a cyber-attack** through an incident response plan, focusing on the legal framework surrounding such attacks. This includes data breach notification requirements, both domestic and international, and an overview of evolving cyber-related legislation. We also explore the legal obligations of organizations, highlighting potential liabilities and consequences of non-compliance.

The session also emphasizes the role of **digital forensics** in incident response and legal proceedings, including best practices for preserving electronic evidence, ensuring its admissibility, and working with law enforcement. Additionally, we cover the **post-incident phase**, discussing breach disclosure, communication strategies, and managing reputational damage. **Practical advice** on engaging regulatory bodies, law enforcement, and legal counsel ensures a coordinated, lawful response to cyber incidents.

To conclude, we get **a firsthand account** from a company (TVH) that has experienced a cyberattack and that has been through the challenges of post-attack damage control.

For this session, no technical prior knowledge/background is needed.

Session 8: Post-quantum cryptography

18 November 2025 - Eric Michiels (IBM)

Even though Quantum Computing systems are not yet powerful enough today to pose a real threat to our cryptography, criminal organisations are suspected of applying the principle of '**harvest today, decrypt later**,' with all the dangers it poses to our critical infrastructure, official contracts, digital signatures, news reliability, and other vulnerabilities. In this session, we delve into '**Quantum-Safe' and 'Post-Quantum Cryptography'** as defensive measures against these threats, which receive significant attention, particularly in the financial, telecommunications, energy, and government sectors. We explain how to establish a '**Quantum-Safe Implementation' project** and which **state-of-the-art technologies** can lend a hand in this process.

This session is aimed at IT professionals and developers.

Practical

When and where?

- 11 February, 11 March, 22 April, 13 May, 10 June, 9 September, 14 October, and 18 November 2025
- All sessions take place from 14:00 - 17:00
- KU Leuven - Campus Rabot (Gebroeders de Smetstraat 1, 9000 Gent).

Registration

- Register online before 04/02/2025
- The fee for the series is € 1650. If you enrol as a company for the whole series, you have the flexibility to send a different employee to each session.
- The cost per session is € 260. The deadline for registration is 5 working days before each session.
- Pay by bank transfer to account number IBAN BE31 2850 2133 2955 of PUC - KU Leuven Continue, stating '400/0026/67943 + name of participant(s) and do not receive an invoice.
- If you would like an invoice, please indicate this when registering.

- NEW: SME-wallet: Increased support for energy transition and cybersecurity
- Starting April 1, 2023, small and medium-sized enterprises (SMEs) can receive a higher percentage of support for training or advice within the theme of 'cybersecurity'. Small enterprises will receive 45% support, while medium-sized enterprises will receive 35%.

PUC - KU Leuven Continue

KU Leuven Kulak
E. Sabbelaan 53 bus 7643 - 8500 Kortrijk
+32 56 24 61 84 - puc@kuleuven.be
puc.kuleuven.be