postuniversitair centrum

Cybersecurity excellence series

KU Leuven Gent

28 February - 23 October 2024

KU LEUVEN KULAK GENT BRUGGE

Scope and overview

In an increasingly technology-driven world, cybersecurity stands as the cornerstone of digital resilience. In this program, we will explore the full spectrum of cybersecurity, from prevention to response, while gaining both immediate, hands-on skills and a foresight for the future of cybersecurity. This program 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 **seven 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 program then progresses to hands-on workshops: one focused on network security (session 3) and another on the protection of the growing category 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 6). Finally, we look ahead to what **the future** holds, especially in the context of cybersecurity in the era of quantum computing (Session 7).

Target audience

This program is tailored for professionals looking to deepen their (technical) knowledge in various aspects of cybersecurity/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.

Programme

28 February 2024 - Vincent Naessens (KU Leuven) |

Session 1: Tackling cybersecurity challenges: a complex security puzzle

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.

26 March 2024 - Kim Wuyts (PwC) |

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

- 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.

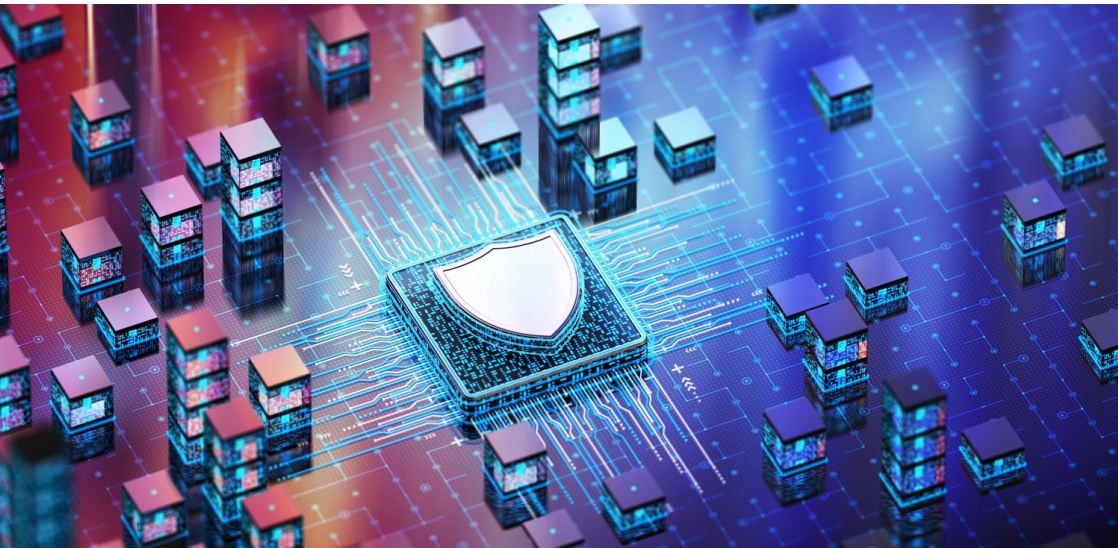
24 April 2024 - Tom Cordemans (KU Leuven) |

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

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.).



29 May 2024 - Jorn Lapon (KU Leuven) |

Session 4: Hacking and protecting embedded devices (workshop)

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.

28 August 2024 - Vincent Naessens (KU Leuven) |

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

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.

25 September 2024 - Tom Bauwens (Eubelius), Kalman Tiboldi (TVH) |

Session 6: Cyberattack response

In this session, we provide a comprehensive guide on effectively responding to cyber-attacks **within the bounds of the law**. The presentation explores the intricate web of **legal considerations** that accompany cyber incidents, delving into the realms of criminal law, data protection, privacy laws, and regulatory compliance together with all other possible side effects.

We begin by dissecting the anatomy of a cyber-attack through **an incident response plan.** A significant portion of the lecture is dedicated to **the legal framework** surrounding cyber-attacks. This includes an examination of data breach notification requirements, both domestically and internationally, as well as an exploration of the evolving landscape of cyber-related legislation. The discussion extends to the legal obligations imposed on organisations, shedding light on potential liabilities and consequences for non-compliance.

Furthermore, the lecture addresses, upon experiences learned, the critical role of **digital forensics** in incident response and legal proceedings. We gain an understanding of **best practices for preserving electronic evidence**, ensuring its admissibility in court, and collaborating with law enforcement agencies.
The lecture also focuses on **the post-incident phase**, elucidating the legal aspects of breach disclosure, communication strategies, and managing reputational fallout. Practical guidance on engaging with regulatory bodies, law enforcement, and legal counsel is provided, offering a roadmap for a coordinated and 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.

23 October 2024 - Eric Michiels (IBM) |

Session 7: Post-quantum cryptography

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?

- Sessions take place at KU Leuven - Campus Rabot: Gebroeders de Smetstraat 1, 9000 Gent
- 14:00 - 17:00
- February 28, March 26, April 24, May 29, August 28, September 25 and October 23, 2024

Language

All sessions will be conducted in English, including lecture materials.

Price

- The fee for the entire program is €1250 for the whole series, or €250 per session. If you enroll as a company for the whole series, you have the flexibility to send a different employee to each session.
- Save on your participation costs via the kmo-portfolio. Our approval number is DV.O102270

Postuniversitair Centrum

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