PwC Cybersecurity and Privacy Day 2024

Description of workshops

Wednesday 5 June 2024

Microsoft Copilot for Security – Defense at machine speed

Bart Bruninx, *Sr. Technical Advisor, Microsoft*

During the workshop you will learn how Microsoft Copilot for Security, an AI-powered cloud-based security analysis tool, can support you in end-to-end scenarios such as incident response, threat hunting, intelligence gathering, and posture management to stay ahead of cyber adversaries.
(#cybersecurity #technical workshop)

Robustness Testing as a Major Challenge in EU AI Act Compliance Assessment

Maxime Cordy, *PhD: Permanent Research Scientist, SnT, University of Luxembourg*
Thibault Simonetto, *PhD Student, SnT, University of Luxembourg*
Luc Stebens, *R&D Engineer on applied ML, SnT, University of Luxembourg*

With the EU AI Act, regular testing of high-risk AI systems will become mandatory in early 2026. According to a study conducted by the EU commission, the total annual compliance costs of a single AI Unit will amount to approximately 29.3k EUR, of which 37% originate from Accuracy and Robustness testing. Although it constitutes a sizeable part of the testing procedure, robustness testing in particular is not thoroughly understood in industry and even lacks a formal definition in the research realm. In our workshop, we will share our definition of robustness based on our research and describe the vulnerabilities AI systems face due to robustness-related challenges. Then, we will explore various strategies to bolster the resilience of AI systems against such threats. To conclude, we introduce a prototype of an in-house developed end-to-end solution to test the robustness of deployed systems and detect vulnerabilities.
(#cybersecurity #technical workshop)

Cost-effective security: unlocking the power of agility

Dennis Schouten, *Co-founder – Sales/Marketing, Chunk Works*
Bas van Sambeek, *Strategy/Communication, Chunk Works*
Peter Willemsen, *Co-founder – Lead developer, Chunk Works*

- **Overview of our technology: briefly describe the functionality of the technology and the specific problems its addresses.**
- **Live demonstration of network decentralization: Peter will present a real-time demonstration where an independent network of nodes transitions into a decentralized network, illustrating the process and the key features.**
- **Resilience demonstration: Simulating the deletion of files/chunk within the network and demonstrate the system's capability to rapidly restore them, showing the speed and efficiency of the self-healing mechanism.**
- **Exploring crypto-agility: Walk through crypto-agility. Peter will explain his reasoning why he built the system like this and how it allows for seamless transition between crypto algos, keys and protocols.**
- **Hybrid PKI overview and future directions: Introduces the concept of hybrid PKI utilized in our technology, detailing the benefits and if time outlining future developments planned."**

(#cybersecurity #technical workshop)

AI in Cybersecurity - Guarding against Intelligent Threats

Dr. Saharnaz Dilmaghani*, Senior Associate Artificial Intelligence & Data Science, PwC Luxembourg*
Vincent Garnier-Salvi*, Senior Manager, Cybersecurity Senior Manager, PwC Luxembourg*

The workshop will focus on the role of AI in enhancing threat detection and the challenges of AI-driven threats. We'll discuss Responsible AI practices as a holistic approach to mitigate these risks and discuss the EU AI Act as the first regulatory framework, guiding you through the complexities of this evolving field.
(#cybersecurity)

Regulatory considerations for digital innovation in a cyber resilient environment

Xiaoyi Fang*, Senior Manager, Regulatory & Compliance, PwC Luxembourg*
Maxime Pallez, *Cybersecurity Director, Cybersecurity Governance, Risk & Compliance Leader*
Vojtech Volf*, Manager, ICT Regulatory and Compliance, PwC Luxembourg*

Let's delve into the regulatory landscape, with a spotlight on the Cyber Act and the Cyber Resilience Act, respectively aiming at enhancing cybersecurity and cyber resilience within the European Union and designed to safeguard consumers and businesses using products or software with digital components.
(#cybersecurity)

The latest news from the CNPD

Alain Herrmann, *Data Protection Commissioner, CNPD*

Discussions with a CNPD Commissioner on the latest topical data protection issues.
(#privacy)

Decoding the AI Act and the risk assessment : What you need to know

Nicolas Hamblenne, *Counsel, PwC Legal Luxembourg*
Audrey Rustichelli, *Partner - Head of Technologies & IP, PwC Legal Luxembourg*

- **Introduction to the EU AI Act (scope, objective, importance, etc).**
- **Key obligations under the AI Act (transparency, data governance, human oversight).**
- **Classification of AI Systems (AI Act's approach to categorizing AI systems based on their risk levels).**
- **Comparing risk assessments (AI >< GDPR).**
- **Next steps & preparing for compliance (key recommendations, updating documents/processes, review contracts, etc).**

(#privacy)

Meet the pitching finalists

Do you want to discover how the solutions selected for the PwC Cybersecurity & Privacy Day are shaping future trends? Curious about how they can bring value to your organisation? Seize the opportunity to meet them and share experiences.
(#cybersecurity #privacy)

pwc