World Institute for Nuclear Security

In partnership with Canada

International Best Practices Workshop on the Role of Advanced Technologies in Effective Cybersecurity at Nuclear Facilities

3–5 February 2026. Vienna, Austria

Day 1: Understanding the Threat Landscape & Cybersecurity Fundamentals

09:00 – 10:30 **Introduction session**

- Welcome and opening remarks
- Workshop objectives and agenda
- Overview of cybersecurity challenges in the nuclear sector and the impact of technologies

10:30 – 10:45 **Coffee Break**

10:45 – 12:30 **Session 1: Current Cyber Threat Landscape**

- OT-targeted attacks
- Supply chain vulnerabilities
- Insider threats

12:30 – 13:30 **Lunch**

13:30 – 15:00 **Session 2: Technology Overview – AI, ML, and Automation in Cybersecurity**

- Key concepts and their role in modern threat detection
- Benefits and limitations in nuclear settings

15:00 – 15:30 Coffee Break

15:30 – 17:00 **Breakout Discussion: Cybersecurity Maturity in Participants' Organizations**

- Sharing of current practices and gaps
- Use of interactive electronic voting for anonymous input

17:00 – 17:30 **Wrap-up and main take-aways of Day 1**

17:30 – 19:00 Workshop reception

Day 2: Applied Technologies and Case Studies

09:00 – 10:30 **Session 3: Advanced Security Architectures – Zero Trust, SOAR, XDR**

- Definitions and core principles
- Relevance and implementation challenges in nuclear environments

10:30 – 11:00 Coffee Break

11:00 – 12:30 **Case Studies – Technology Integration at Nuclear Facilities**

- Real-world examples from nuclear operators and other critical infrastructures

12:30 – 13:30 Lunch

13:30 – 15:00 **Panel Discussion: Cross-Sector Lessons Learned**

- Insights from energy, transport, and financial sectors
- Q&A with technology vendors and operators

15:00 – 16:30 Coffee Break

16:30 – 17:30 **Breakout Session: Identifying Immediate Cybersecurity Improvements**

- Participants collaborate to define practical steps for their organizations

17:30 – 19:30 **Vendor Session: Participants can assist to vendor demos and engage in one-to-one discussions with them**

Day 3: Strategic Planning and Future Outlook

09:00 – 10:30 **Session 4: Cyber Resilience Planning at National and International Levels**

- National strategies and international cooperation
- Role of law enforcement and technical support organizations
- IAEA guidance and global perspectives
- Regulatory compliance and operational resilience

10:30 – 11:00 Coffee Break

11:00 – 12:30 **Session 5: Skills, Workforce, and Diversity in Cybersecurity**

- Building capacity in nuclear cybersecurity
- Promoting female participation and leadership

12:30 – 13:30 Lunch

13:30 – 15:00 **Workshop next steps: Action Planning & Commitments**

- Participants identify next steps for implementation
- Use of online polling to gather commitments and feedback

15:00 – 15:30 Coffee Break

15:30 – 16:30 **Closing Session: Summary, Reflections, and Way Forward**

- Workshop highlights
- Final remarks and closing