Doc for trainers

Planning

24 august	25 august	26 august	27 august	28 august
	Christophe Gransart What are the main tools of the criminals? Which tools for which wireless technology?	**Paul Monferran** Attack Detection	**Dalibor Dolezal** How the different human-being features can be combined with the advanced technological characteristics?	**Martin Griesbacher** Human factors in Cybercrime
	Christophe Gransart Attack test bench: WiFi	**Rasa Brūzgienė** Table-top risk management game "NOrisk"	**Dalibor Dolezal** How the different human-being features can be combined with the advanced technological characteristics?	**Marcel Moritz** From the NIS Directive to the Cyber Resilience Act: how the European Union is integrating cybersecurity to combat cybercrime
Lunch time	Lunch time	Lunch time	Lunch time	Lunch time
Valeria Loscri Introduction of the summer Week Presentation des intervenants	**Virginie Deniau** Attack test bench: 5G	**Rasa Brūzgienė** Table-top risk management game "NOrisk"	**Antoine Gallais and Jerome Ridet** OSINT Open Source Intelligence	
Virginie Deniau We start by the techno.. An overview of Wireless Technology and examples of attacks	**Virginie Deniau and Christophe Gransart** Attack test bench: LoRa	Visit of the lille center	Pitch of participants to the summer school	

AGENDA

DAY 1 (24.08.2026)

13.30 - 14.00 *Arrival and registration of the participants*

14.00 - 14.30 ***Welcoming remarks by organizers Valeria Loscri, Virginie Deniau, Christophe Gransart***

14.30 - 18.00 ***Virginie Deniau, Christophe Gransart***

We start by the techno..

An overview of Wireless Techno and examples of attacks

Theoretical and practical aspects of wireless networks

DAY 2 (25.08.2026)

09.00 - 10.30 ***Christophe Gransart, Badreddine El Bousty***

What are the main tools of the criminals? Which tools for which wireless technology?

10.30 - 11.00 *Coffee break*

11.00 - 12.30 ***Christophe Gransart, Badreddine El Bousty***

Attack test bench: Wi-Fi

12.30 - 14.00 *Lunch break*

14.00 - 15.30 ***Virginie Deniau***

Attacks on test bench : 5G

15.30 -16.00 *Coffee Break*

16.00 - 17.30 ***Virginie Deniau, Christophe Gransart***

Attacks on test bench : LoRa

17.30 - 18.00 ***Concluding remarks***

DAY 3(26.08.2026)

09.00 -10.30 Jonathan Villain

Attacks Detection

10.30 -11.00 *Coffee Break*

11.00 -12.30 Rasa Brūzgienė and Šarūnas Grigaliūnas (Kaunas University of Technology, Department of Computer Sciences, Lithuania)

Table-top risk management game "NOrisk"

Table-top risk management game "NOrisk"
This course centers on an interactive table-top simulation game aimed at strengthening practical skills in cyber risk identification, assessment, and response planning. Participants engage in realistic, human-centric cybercrime scenarios and apply the method in a role-based setting. Players are assigned organizational roles—IT/security specialists, officers (e.g., CISO, DPO), or employees—and provided with a detailed company profile, threat documentation, evidence, and role-specific guidance. The game is built around two scenarios: (1) a tailgating attack involving unauthorized physical access and malicious package delivery, and (2) a social engineering attack combined with a wireless IoT compromise. Within their roles, participants identify threats and vulnerabilities, assess human-factor impacts, evaluate existing controls, analyze risks, and develop prioritized mitigation and risk-management actions.

12.30 - 14.00 Lunch break

14.00 - 15.30 Rasa Brūzgienė and Šarūnas Grigaliūnas (Kaunas University of Technology, Department of Computer Sciences, Lithuania)

Table-top risk management game "NOrisk"

15.30 – 16,000 Coffee Break

Visit of the Lille center

DAY 4(27.08.2026)

09.00 - 12.30 Dalibor Dolezal

how the different human-being features can be combined with the advanced technological characteristics?

12.30 - 14.00 Lunch break

14.00 - 15.30 Antoine Gallais and Jerome Ridet

OSINT : Open Source Intelligence

15.00 - 15.30 Coffee Break

16.00 - 17.30 **Pitch of participants to the summer school**

DAY 5(28.08.2026)

9.00 - 10.30 Martin Griesbacher

Human factors in Cybercrime

10.30 - 11.00 Coffee Break

11.00 - 12.30 Marcel Moritz

From the NIS Directive to the Cyber Resilience Act: how the European Union is integrating cybersecurity to combat cybercrime

Abstract: In less than 10 years, the European Union has developed an impressive arsenal of regulations to enforce stricter cybersecurity requirements. In doing so, it has given rise to new measures that represent economic opportunities for cybersecurity professionals, particularly in the field of IoT.

12.30 - 13.00 Distribution of certificates and Concluding Remarks