CyberEM - Cybercrime from the techno to the crime

Training School

24 - 28 August 2026

Venue in Villeneuve d'Ascq

Venue: University Gustave Eiffel,

20 rue Elisee Reclus

59650 Villeneuve d'Ascq

France

Google Maps:

https://www.google.com/maps/place/20+Rue+%C3%89lis%C3%A9e+Reclus,+59650+Villeneuve-d'Ascq/@50.6080802,3.1322367,16z/data=!3m1!4b1!4m6!3m5!1s0x47c2d64563136da5:0x678e8756e80d29ef!8m2!3d50.6080802!4d3.1322367!16s%2Fg%2F11mcy9sq3c?entry=ttu&g_ep=EgoyMDI2MDQwNS4wIKXMDSoASAFQAw%3D%3D

Room: Europe

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 ***Virginie Deniau, Christophe Gransart, Badreddine El Bousty***

Social engineering in the criminal process

Practical works with techno for cyber crime

10.30 - 11.00 *Coffee break*

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

What are the main tools of the criminals?

Which tools for which technology?

12.30 - 14.00 *Lunch break*

14.00 - 15.30 ***Christophe Gransart, Badreddine El Bousty***

Attacks on Wi-Fi test bench

15.30 -16.00 *Coffee Break*

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

Attacks on 5G test bench

17.30 - 18.00 ***Concluding remarks***

DAY 3(26.08.2026)

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

Attacks on Lo-Ra test bench

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

Table-top risk management game "NOrisk"

15.00 - 15.30 Coffee Break

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 **Attack detection using ML**

Christophe Gransart, Paul Monferran

15.00 - 15.30 Coffee Break

16.00 - 17.30 **TBD**

Martin Griesbacher (to be confirmed)

DAY 5(28.08.2026)

9.00 - 10.30 **TBD**

Martin Griesbacher (to be confirmed)

10.30 - 11.00 Coffee Break

11.00 - 12.30 From the NIS Directive to the Cyber Resilience Act: how the European Union is integrating cybersecurity to combat cybercrime

Marcel Moritz

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

Microsoft Teams Need help?

Join the meeting now

Meeting ID: 377 535 422 825 0

Passcode: JC9vB3bM