Cybersecurity and its multifaceted aspects

Training School

7 - 11 September 2026

Split, Croatia

https://www.efst.unist.hr/en/

Venue: *University of Split, Faculty of Economics, Business and Tourism, Cvite Fiskovića, 5, 21000 Split, Croatia*

Google Maps: https://maps.app.goo.gl/V3313wUGVHwtRKbo7

Room: RC - TBC

AGENDA

DAY 1 (07.09.2026)

13.30 - 14.00 *Arrival and registration of the participants*

14.00 - 14.30 ***Welcoming remarks by organizers***

14.30 - 16.00 ***Invited speakers***

***Marko Čular* - Foundations of Modern Cybersecurity - Introductory part - Who Truly Owns Cyber Risks**

Cyber risks are no longer solely the responsibility of IT but have become an integral part of overall risk management and an organization's strategic resilience. The lecture presents cyber risk management through the Three Lines Model: IT management manages and implements controls, the CISO provides expert support and oversees their effectiveness, while Internal Audit provides independent assurance to the Board. Executive management, which ensures the necessary resources and strategy, and the Board, which sets the "tone from the top" and oversees the overall risk management system, also play a key role.

16.00 -18.00 ***Josip Musić - Digital Dalmatia, a County Technology Hub***

This session introduces Digital Dalmatia, a County Technology Hub dedicated to promoting and developing the IT/tech sector across Split and the Dalmatia region. Participants will get an overview of its three main focus areas - digital skills, startup ecosystem, and tech community. The talk offers international researchers and professionals a window into how a regional public initiative is working to position itself as a recognized stakeholder in Europe's tech landscape.

DAY 2 (08.09.2026)

09.00 - 10.30 ***Mislav Kovač* - Human Factors and Usability in Cybersecurity**

Focusing on the role of human behavior in security incidents, this topic examines how users, administrators, and decision-makers interact with security technologies. It addresses issues such as social engineering, insider threats, security awareness, and usability, highlighting how human-centered design can significantly improve security outcomes.

10.30 - 11.00 *Coffee break*

11.00 -12.30 ***Mislav Kovač* - Human Factors and Usability in Cybersecurity** *(Continued)*

12.30 - 14.00 *Lunch break*

14.00 - 15.30 ***Saša Bilić* - Cybersecurity in Industrial and Critical Infrastructures**

This topic explores cybersecurity challenges in industrial environments, including critical infrastructure, operational technology (OT), and cyber-physical systems. Participants will learn about sector-specific risks, legacy systems, safety-security interactions, and incident response in high-impact environments where failures can have societal consequences.

15.30 -16.00 *Coffee Break*

16.00 - 17.30 ***Saša Bilić* - Cybersecurity in Industrial and Critical Infrastructures** *(Continued)*

17.30 - 18.00 ***Panel Discussion and Concluding remarks***

DAY 3 (09.09.2026)

09.00 - 10.30 ***Ivan Chorbev* - AI and Data-Driven Approaches in Cybersecurity**

Participants will examine how artificial intelligence and machine learning are used to support cybersecurity tasks such as threat detection, anomaly detection, and incident response. The topic also addresses limitations, risks, and trust issues related to AI-based security solutions, emphasizing the need for transparency, robustness, and responsible deployment.

10.30 - 11.00 *Coffee break*

11.00 -12.30 ***Ivan Chorbev* - AI and Data-Driven Approaches in Cybersecurity** *(Continued)*

12.30 - 14.00 *Lunch break*

14.00 - 15.30 ***Salko Kovačić* - Privacy, Ethics, and Responsible Cybersecurity**

This topic introduces ethical principles and privacy considerations relevant to cybersecurity practice and research. It covers topics such as data protection, surveillance, proportionality, bias, accountability, and the societal impact of security technologies, encouraging participants to integrate ethical reasoning into technical decision-making.

15.30 -16.00 *Coffee Break*

16.00 - 17.30 ***Gurjot Singh GABA* - Governance, Regulation, and Cyber Risk Management**

Participants will explore how cybersecurity is shaped by legal frameworks, standards, and organizational governance structures. The topic covers risk assessment, compliance, policy development, and regulatory instruments, helping participants understand how technical solutions align with legal and organizational requirements.

17.30 - 18.00 ***Panel Discussion and Concluding remarks***

DAY 4 (10. 09. 2026)

09.00 - 10.30 ***Sonay Caner-Yıldırım* - Intersectionality by Design in Cybersecurity: From Awareness to Research Practice**

This session explores how intersectional factors can be recognized and meaningfully integrated into cybersecurity research and design. Drawing on examples from gender sensitive and intersectional cybersecurity studies, it moves from awareness of overlapping forms of exclusion to practical research decisions involving participants, methods, data, design, and evaluation.

10.30 - 11.00 *Coffee break*

11.00 -12.30 ***Elva Leka* – Human-Centric Cybersecurity in Practice: Investigating Cyber Incidents and Insider Threats**

This interactive session explores the human dimension of cybersecurity through a practical, team-based exercise. Participants will investigate a simulated cybersecurity incident, analyse the available information, identify potential security risks, and apply critical-thinking and problem-solving skills. The session concludes with a joint discussion of the findings, possible response strategies, and key lessons learned.

12.30 - 14.00 *Lunch break*

14.00 - 15.30 ***Živko Krstić* - Emerging Threats and Future Directions in Cybersecurity**

The final topic looks ahead to emerging trends and challenges, including supply-chain attacks, AI-enabled threats, misinformation campaigns, and security implications of future digital infrastructures.

Participants will be encouraged to critically assess future risks and identify research and innovation directions in cybersecurity.

15.30 -16.00 *Coffee Break*

16.00 - 17.30 ***Živko Krstić* - Emerging Threats and Future Directions in Cybersecurity** *(Continued)*

The final topic looks ahead to emerging trends and challenges, including supply-chain attacks, AI-enabled threats, misinformation campaigns, and security implications of future digital infrastructures. Participants will be encouraged to critically assess future risks and identify research and innovation directions in cybersecurity.

17.30 - 18.00 ***Panel Discussion and Concluding remarks***

DAY 5 (11. 09. 2026)

***09.00 -10.30 Trainees* Presentation Session and Discussion (All Trainees and Mentors)**

10.30 -11.00 Coffee break

***11.00 - 12.00* Trainees Presentation Session and Discussion (All Trainees and Mentors)**

12.00 - 12.30 Distribution of certificates and Concluding Remarks