MONTHLY BULLETIN

NOVEMBER 2025

CONTENT

- Western Balkans in Focus: Strengthening Capacities for Identifying and Countering Hybrid Threats
- From Response to Prevention: The New National Approach to Cyber Risk Management
- AKSK places the focus on intelligent testing and early vulnerability assessment
- 41 high-school senators trained on cyber hygiene
- Universities at the Center of the New Program for Developing Cybersecurity Talent
- Five-day training by SEI to enhance institutional capacities in cyber risk assessment

Western Balkans in Focus: Strengthening Capacities for Identifying and Countering Hybrid Threats

The Conference and Hybrid Threat Simulation Exercise in the Western Balkans, organized in Tirana by the Hybrid CoE in cooperation with AKSK, brought attention to the dynamics of hybrid threats affecting the region. Experts from Euro-Atlantic institutions, government representatives, academics, and security professionals discussed the tactics used by malicious actors, the challenges facing the region, and the coordinated measures needed to respond effectively.

The Director General of AKSK, Igli Tafa, emphasized that hybrid threats require an integrated approach that combines analysis, technology, awareness, and regional cooperation. He underlined that strengthening national and regional capacities, information sharing, and establishing rapid response mechanisms are essential to ensure the region's security and strategic resilience against destabilizing activities.

From Response to Prevention: The New National Approach to Cyber Risk Management

AKSK presented the unified national approach to cyber risk management during an event attended by public institutions, essential service operators, and critical information infrastructure entities. The session outlined the standardized methodology that guides institutions in identifying, assessing, and addressing risks, creating a common foundation for decision-making and strategic planning.

The Director General of AKSK, Igli Tafa, emphasized that transforming institutional culture from incident response to proactive prevention is essential for a resilient cyber environment. He highlighted that implementing the new methodology and strengthening the practical capabilities of institutions are key elements for effectively confronting emerging threats and ensuring digital security at the national level.

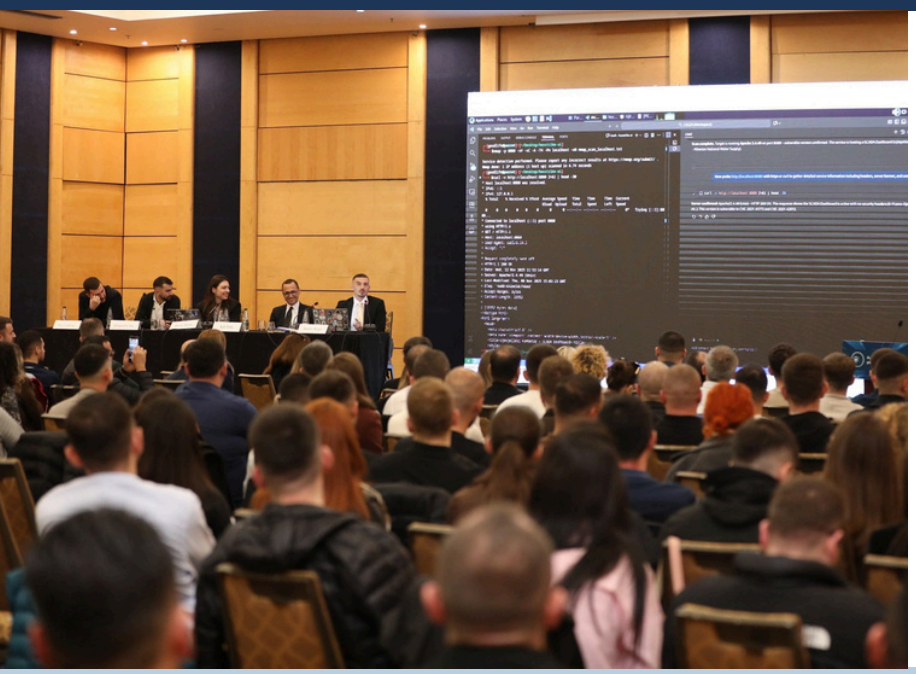
Address : Rruga "Papa Gjon Pali II", Nr. 3, Kati I Tiranë

www.aksk.gov.al

@aksk.gov.al

+355 422 21 039

NOVEMBER 2025



AKSK places the focus on intelligent testing and early vulnerability assessment

As part of the ongoing series of meetings with operators of critical and important information infrastructures, the National Cyber Security Authority held the third technical session titled “Proactive Monitoring and Simulation”, with the participation of around 250 representatives. During the opening remarks, the Director General of AKSK, Igli Tafa, emphasized that cybersecurity must be grounded in foresight and prevention, highlighting the role of knowledge, training, and professional expertise in strengthening institutional capacities.

The event featured the presentation of the national platform for penetration testing, which leverages artificial intelligence to identify and analyze vulnerabilities in digital systems. The role of Red Team operations and new approaches to cross-sector collaboration were also discussed. This initiative is part of the “AKSK ProActive 2026” program, which aims to reinforce the preventive approach and build a resilient national cybersecurity ecosystem.

Good Cyber Governance: A Priority for Critical and Important Information Infrastructure

The National Cyber Security Authority organized a training session with 41 high-school senators, focusing on cyber hygiene and building safe practices in the digital environment. The activity presented the main online risks affecting young people, methods for identifying online scams, and protective measures for personal and data security.

The training aimed to raise awareness and strengthen the role of youth as promoters of digital safety within their school communities. AKSK highlighted the importance of early education and the active involvement of the younger generation in building a resilient cyber culture, emphasizing that investing in their knowledge represents an important pillar of national security.

Universities at the Center of the New Program for Developing Cybersecurity Talent

The National Cyber Security Authority held a meeting with rectors, university representatives, and the Deputy Minister of Education, where CRDF Global presented a four-year project supported by the U.S. Department of State, aimed at enhancing technical and academic capacities in the field of cybersecurity. The project seeks to align university programs with the real demands of the labor market and strengthen the role of higher education institutions in developing national digital capacities.

The program includes a package of strategic interventions, such as training the trainers, developing practical modules, and reviewing higher education policies, with the goal of enabling universities to build functional structures that can, in the future, provide SOC-type training and services. The meeting served to define the first steps of implementation, laying the foundation for sustainable collaboration between AKSK, universities, and international partners in building a cybersecurity talent ecosystem.

Five-day training by SEI to enhance institutional capacities in cyber risk assessment

The Software Engineering Institute (SEI) at Carnegie Mellon University, in collaboration with the U.S. Department of State and AKSK, conducted a five-day training dedicated to the staff of AKSK, AKSHI, and institutions involved in the national cyber risk assessment process. The program focused on enabling participants to analyze and utilize the results of cybersecurity assessments, with the aim of identifying critical risks and implementing the necessary controls to strengthen institutional protection.

During the opening of the event, the Director General of AKSK, Igli Tafa, acknowledged the mutual support of the U.S. Department of State and the expertise of SEI, emphasizing their role in enhancing technical capacities and promoting a proactive approach to risk management. Throughout the program, participants worked with specialized modules on assessment approaches, the use of standards, interpreting results, and defining institutional responsibilities, concluding with concrete recommendations to strengthen security processes.