05 July, 2024

Model for Cybersecurity Exploration in Educational Institutions in Plovdiv through IICT-BAS Branch

Authors:

Tiana Kaleeva, PHD

Peyo Staribratov

Denis Petkov

Authors

Tiana Kaleeva, PhD

Peyo Staribratov

Denis Petkov

Report topic

The report presents a model for cybersecurity exploration, influenced by the Cyber4All Star Project in line with the European Digital Innovation Hub “Trakia”’s impact over the stakeholders and outlines the significant role of the establishment of a IICT-BAS Branch as a collaborator between the Hub and the educational institutions.

Cyber4All Star Project

The project offers expertise access to cybersecurity services, finance and ecosystem networking with technology suppliers in line with the European Digital Innovation Hub “Trakia”. The hub in collaboration with other Cybersecurity EDIHs across Europe via the European Corridor of Cybersecurity EDIHs offers a full range of Cybersecurity services to stakeholders with a special focus on SMEs, mid-caps and PSOs.

CYBER
4 ALL STAR

Importance of Cybersecurity Training

Threats

Employees recognize and respond to potential threats like phishing, malware, and social engineering. By understanding these threats, stakeholders can take proactive measures.

Compliance

Cybersecurity training ensures that employees are aware of and adhere to legal requirements, helping organizations avoid hefty fines and legal consequences.

Security-First Culture

Employees understand the importance of cybersecurity and their role in maintaining it.

Cybersecurity Brokers

Personalized Recommendations

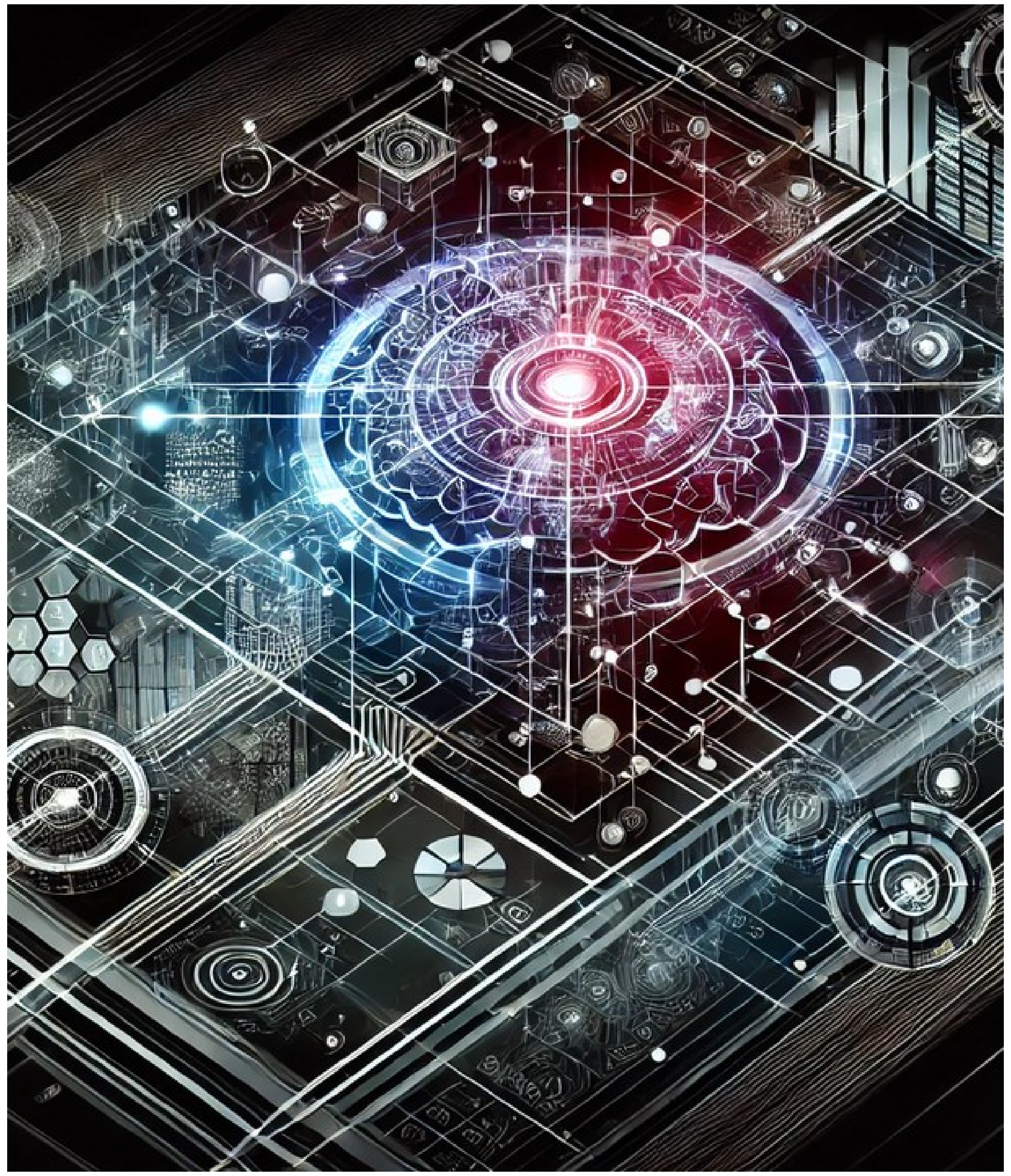
Ongoing Assessment

Communication Bridge

Cognitive Security

The cognitive security is an essential aspect of cybersecurity, aiming to protect cognitive processes and information integrity from malicious interference.

In educational institutions, it provides safeguards to the students and administrative personnel against misinformation and psychological manipulation, ensuring a secure and trusted learning environment.



Critical Infrastructure Protection

Research and development activities in the system of BAS and the educational institutions are considered of strategic importance, potentially affecting different elements of the national critical infrastructure.

In some cases, the collaboration with the defense and security sector might require the involvement of critical infrastructure's operators or stakeholders, outlining the significant importance of its protection.

Conclusion

By developing a Model for Cybersecurity Exploration in Educational Institutions, we aim to enhance their cybersecurity culture, understanding and sustainability against malicious interference.

Thank you for your attention!