**BUILDING A VIRTUAL CYBER POLYGON ENVIRONMENT**

**Imamverdiyev Yadigar Nasib, Gasimli Farid Fikret, Sadigzade Jafar Zafar**

*Azerbaijan Technical University, Baku, Azerbaijan*

[*yadigar.imamverdiyev@aztu.edu.az*](mailto:yadigar.imamverdiyev@aztu.edu.az)*,* [*farid.gasimli@aztu.edu.az*](mailto:farid.gasimli@aztu.edu.az)*, jafarsadigzade@gmail.com*

**Summary:** In today's age, almost every day we come across new cyber attack methods and techniques. Although research is being conducted at the level of both the government and some cyber security companies to study and prevent these cyber attacks, it is difficult for other people in this field to engage in research in this field without a real work environment. For this reason, no matter how much cyber security is developing, cyber security science and research in this field lags far behind. In the article we have written, a new virtual cyber polygon environment has been built to increase scientific-practical research in the field of cyber security, as well as to make the results of the studies closer to reality, and suggestions have been made for the exploitation of this environment.

**Keywords:** Security operations center, SOC, security solutions, security tools, cyber security lab, CTF

1. **Introduction**
2. **Generic cyber polygon model**
3. **Hybrid architecture of CP**
4. **Components of CP**
5. **Physical and virtual CP environments**
6. **Emulation and simulation environments**
7. **CP environments used**
8. **Use of CP training and testing environment**
9. **Advantages and disadvantages of CP**
10. **CP architecture based on security operations center**

**Conclusion**

**Reference**

1. Tsurkan, Vasyl, and Valeriia Pokrovska. "Analysis of cyber exercises approaches." *ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ І БЕЗПЕКА* (2020): 169.
2. Pandey, Bishwajeet, and Shabeer Ahmad. *Introduction to the Cyber Ranges*. Chapman and Hall/CRC, 2022.
3. Katsantonis, Menelaos N., Athanassios Manikas, Ioannis Mavridis, and Dimitris Gritzalis. "Cyber range design framework for cyber security education and training." *International Journal of Information Security* 22, no. 4 (2023): 1005-1027.
4. Smyrlis, Michail, Konstantinos Fysarakis, George Spanoudakis, and George Hatzivasilis. "Cyber range training programme specification through cyber threat and training preparation models." In *International Workshop on Model-Driven Simulation and Training Environments for Cybersecurity*, pp. 22-37. Cham: Springer International Publishing, 2020.
5. Mahmoud, Rasmi-Vlad, Egon Kidmose, Ahmet Turkmen, Olga Pilawka, and Jens Myrup Pedersen. "DefAtt-architecture of virtual cyber labs for research and education." In *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, pp. 1-7. IEEE, 2021.