Тема: Развој виртуелизоване платформе за емулацију напада и детекцију сајбер претњи

Наставник: Бранко Арсић

Циљ мастер рада је пројектовање, имплементација и експериментална евалуација модуларне лабораторијске платформе за сајбер безбедност, засноване претежно на технологијама отвореног кода. Платформа је замишљена као изоловано, преносиво и поновљиво Cyber Range окружење у којем се могу безбедно извршавати контролисани сценарији напада, прикупљати безбедносна телеметрија, детектовати сумњиве активности и пратити читав ток обраде инцидента. Још један циљ рада је развој функционалног окружења које повезује емулацију нападача, SIEM/XDR аналитику, управљање инцидентима и инфраструктурни мониторинг, уз могућност квантитативног мерења успешности имплементираних безбедносних контрола.

Крајњи резултат рада биће функционална и оперативна Cyber Range платформа, заједно са скриптама за аутоматизацију процеса, конфигурационим фајловима, детекционим правилима, нападачким сценаријима, интеграционим сервисом и методологијом за евалуацију. Овакво окружење може се користити за истраживање, развој и проверу сајбер напада, обуку SOC (Security Operations Center) аналитичара и извођење практичних вежби у контролисаним условима. Главни допринос рада огледа се у обједињавању више фаза животног циклуса безбедносног инцидента у једну модуларну, мерљиву и лако интерпретабилну платформу прилагођену академским и стручним потребама.

Литература:

[1] Yamin, M. M., Katt, B., & Gkioulos, V. (2020). Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. Computers & Security, 88, 101636. https://doi.org/10.1016/j.cose.2019.101636

[3] Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2020). MITRE ATT&CK: Design and Philosophy. The MITRE Corporation. https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf

[4] Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer Security Incident Handling Guide (NIST Special Publication 800-61, Revision 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r2

[5] Manzoor, J., Waleed, A., Jamali, A. F., & Masood, A. (2024). Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs. PLOS ONE, 19(3), e0301183. https://doi.org/10.1371/journal.pone.0301183

[6] The MITRE Corporation. CALDERA: Automated Adversary Emulation Platform [softver i dokumentacija]. https://caldera.readthedocs.io/

[7] Red Canary. Atomic Red Team: Library of Simple, Testable Adversary Emulation Techniques Mapped to MITRE ATT&CK [softver i dokumentacija]. https://github.com/redcanaryco/atomic-red-team

[8] Wazuh Inc. Wazuh: The Open Source Security Platform (SIEM/XDR) [softver i dokumentacija]. https://wazuh.com/