AI4ADAPT Optimizer of incident response adaptation

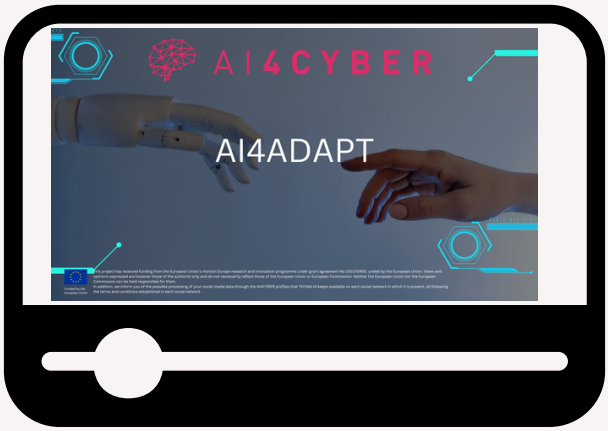
"Intelligent" Reinforcement Learning (RL) solution with the main objective of optimizing the incident response adaptation. The component is designed to defend the victim system against certain types of attacks (advanced attacks in the AI4CYBER nomenclature) which are composed of a chain of different atomic attacks.

AI4CYBER Component

The AI4DAPT solution provides full automation of RL agent training in a realistic environment so that in production the recommended security control action to execute as response to attacks is optimized and adapted to the actual attack step and security status of the system.

AI4ADAPT is a python RL agent and accompanying database and applications aimed at identifying the best defensive actions for the security operator based on the status of the real system.

AI4ADAPT RL agent interacts with the Blue team environment in order to go learning the best safeguard possible according to the monitored real status of the system under attack or incident. AI4ADAPT continuously collects observations related to the security status of the system, processes them, and sends the optimal defence strategy (i.e., set of security controls) for incident response at a given time and status of the system.
The AI4ADAPT architecture is comprised of components for the RL agent training phase, where security event monitoring, the security status computation, and defence execution in the sandboxed environment is performed autonomously by the RL agent. Once the agent is trained, in production phase, however, AI4ADAPT shall work together with Security Orchestration Automation and Response (SOAR) solutions (such as the AI4SOAR component in AI4CYBER framework) and monitoring tools on the critical System under protection to provide recommendations (and not execution) on defensive actions.



YouTube Video Link

The solution is still a prototype and the future tool will have commercial license.

tecnalia
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

Erkuden Rios (Erkuden.rios@tecnalia.com)
Fundación Tecnalia Research & Innovation.

www.tecnalia.com
https://es.linkedin.com/company/tecnalia-research-innovation
https://x.com/tecnalia

E. Iturbe, E. Rios, A. Rego, and N. Toledo, "Artificial Intelligence for next generation cybersecurity: The AI4CYBER framework", in Proceedings of the 18th International Conference on Availability, Reliability and Security, 2023, pp. 1–8.

E. Iturbe, A. Rego, O. Llorente-Vazquez, E. Rios, C. Dalamagkas, D. Merkouris, and N. Toledo, "Reinforcement Learning in action: Powering intelligent intrusion responses to advanced cyber threats in realistic scenarios," Expert Syst. Appl., vol. 2025, Art. no. 129168, 2025.

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070450. Disclaimer: Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Commission. Neither the European Union nor the European Commission can be held responsible for them.