AI4SOAR

AI-powered Security Orchestration, Automation, and Response

AI4SOAR is designed to enhance automated incident response by building upon the existing open-source SOAR platform Shuffle. It employs similarity-learning to dynamically select and adjust appropriate playbooks by comparing new alerts with historical ones, thereby speeding up and improving the accuracy of incident response.

AI4CYBER Component

The AI4SOAR solution provides:

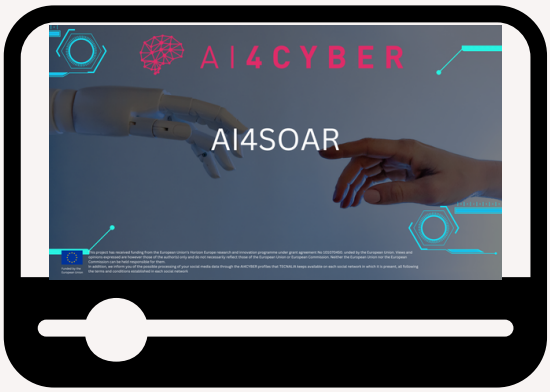
- Faster Response Time: Automation reduces manual workload, significantly cutting down time to detect and mitigate incidents.
- Improved Adaptability: Unlike static playbooks, AI4SOAR dynamically adjusts responses to handle evolving or previously unseen threats.
- Context-Aware Playbook Selection: Uses similarity-based learning to identify the best response based on alert context.
- Seamless Integration: Works with tools like TheHive and Cortex via APIs, enhancing broader security orchestration.

AI4SOAR is an AI-powered extension of Security Orchestration, Automation, and Response (SOAR) platforms, developed by Montimage in the scope of the EU AI4CYBER project.

Instead of relying only on rigid, predefined workflows, AI4SOAR analyzes historical alerts and dynamically matches them with new ones, allowing security teams to automate incident handling in a way that is faster, more accurate, and more adaptable to evolving cyber threats.

Through this approach, AI4SOAR addresses a major challenge in today's security operations: the overwhelming number of alerts and the rigidity of existing automation platforms. It integrates seamlessly with popular security tools such as TheHive and Cortex, enabling security teams to maintain their existing ecosystems while improving response efficiency. By reducing reliance on manual intervention and adjusting responses to novel or sophisticated attacks, AI4SOAR helps organizations cut response times, improve resilience, and better protect critical systems.

The tool has been evaluated in several real-world scenarios, demonstrating its capability to automate both detection and tailored response. Its innovation lies in combining orchestration and AI-driven adaptability, offering a practical step toward more autonomous and intelligent security operations.



YouTube Video Link

TThe solution is still a prototype and the future tool will have commercial license. AI4SOAR is hosted as an open-source project in Montimage GitHub repository under the Apache-2.0 licence. It has also a commercial license for a more commercial version.
https://github.com/montimage/AI4SOAR

Manh Dung Nguyen
(manhdung.nguyen@montimage.eu)
Montimage

https://www.montimage.eu/

Manh-Dung Nguyen, Wissam Mallouli, Ana Rosa Cavalli, Edgardo Montes de Oca "AI4SOAR: A Security Intelligence Tool for Automated Incident Response", In the ARES '24: Proceedings of the 19th International Conference on Availability, Reliability and Security. Pages 1 - 8 https://doi.org/10.1145/3664476.3670450

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.