



AI4DECEIVE

Honeynet deployment platform

The main goal of AI4DECEIVE is the dynamic and intelligent deployment of honeypots throughout a network infrastructure, commonly referred to as honeynet orchestration.



Honeynet deployment strategy decision complexity is automatically handled by the AI4DECEIVE tool while the security operator workload is reduced.



AI4DECEIVE's Intelligent Deceive Decision Engine (IDDE) module applies game theory algorithms to determine the optimal type and number of honeypot instances needed to mitigate detected threats against a system under protection.

The game theory-based models enable modelling attacker-defender interactions, planning deception strategies, and conducting cost-benefit analyses. The solution works together with the Montimage Monitoring Tool (MMT) which enables real-time log processing, threat detection, and visualization to support the computation of the best dynamic deception strategies. MMT has been enhanced to extract additional parameters from network activity, including the specific service being exploited at each step of an attack. The attack information from the MMT is forwarded to the IDDE, allowing it to make smarter informed decisions by mapping attack behaviours to the most appropriate honeypot types.

The Honeypot Manager component, accompanied by the Honeypots Catalogue, covers the deployment needs of each use case scenario, both in type and number of honeypot instances required to lure the attackers, and offering support to hybrid (local and cloud) deployments, as needed.



[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.



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.