AI4TRIAGE

AI-powered Cybersecurity Alert Triage and Root-Cause Analysis Tool

AI4TRIAGE automates the characterization (in terms of MITRE attacks TTPs), triage, categorization, and prioritization of cybersecurity alerts. It leverages AI techniques to assess alert context, determine severity, and identify probable root causes, allowing security teams to handle critical incidents more effectively.

AI4CYBER Component

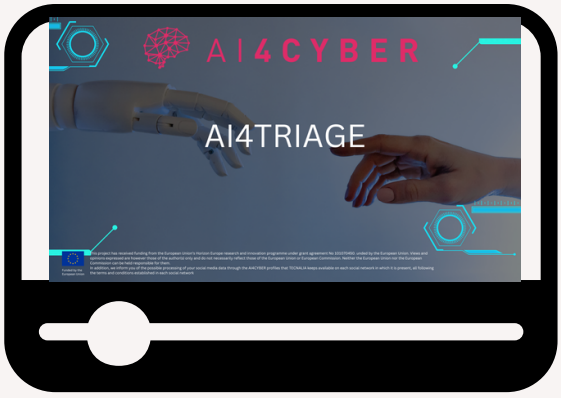
TThe AI4TRIAGE solution provides:

- Prioritization of Critical Alerts: Helps operators to understand the alerts by linking them on the corresponding attacks TTPs and to focus on the most urgent incidents.
- Reduced Alert Fatigue: Decreases the overwhelming workload caused by large volumes of false positives or low-priority alerts.
- Context-Aware Analysis: Provides additional intelligence to support decision-making.

AI4TRIAGE is a cybersecurity triage solution developed under the EU-funded AI4CYBER project to tackle one of the most pressing challenges in security operations: the excessive volume of alerts generated by monitoring systems.

Many existing solutions struggle to separate critical events from noise, resulting in alert fatigue and delayed incident response. AI4TRIAGE applies advanced AI and machine learning algorithms to automatically categorize, score, and prioritize alerts based on contextual information and historical patterns and link them to attack TTPs. This ensures that security teams focus their attention on the most significant threats first.

Beyond classification, AI4TRIAGE performs root-cause analysis to help identify the origin and propagation path of an incident. This context not only accelerates investigation but also improves the next step related to the quality of response and remediation actions. Acting as a bridge between detection mechanisms (e.g., IDS/IPS, SIEM systems) and response tools (such as SOAR platforms), AI4TRIAGE enhances situational awareness, streamlines workflows, and improves resilience. The tool has been designed to integrate seamlessly within the AI4CYBER ecosystem, supporting use cases across domains like critical infrastructures, finance, and transportation. Its adaptability makes it a key enabler for next-generation cybersecurity frameworks where AI-assisted decision-making is essential for keeping pace with evolving threats.



YouTube Video Link

The solution is still a prototype and the future tool will have commercial license. AI4TRIAGE is hosted as an open-source project in Montimage GitHub repository under the Apache-2.0 licence. https://github.com/montimage-projects/AI4TRIAGE

montimage

Maxime Vinh-Hoa La
(maxime.vinhhoa.la@montimage.eu)
Montimage

https://www.montimage.eu/

- Ivan Orefice, Wissam Mallouli, Ana R. Cavalli, Filip Sebek and Alberto Lizarduy Diagnosis Automation using Similarity Analysis: Application to Industrial Systems. in the 19th International Conference on Software Technologies (ICSOFT) proceedings. ISBN 978-989-758-706-1, ISSN 2184-2833, pages 331-338. July 08 - 10, 2024 Dijon, France.
- Training : ARES 2025 : Root Cause Analysis in Cyber Incidents: From Alerts to Actionable Insights – Wissam Mallouli (Montimage, France). https://2025.ares-conference.eu/program/stam/

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.