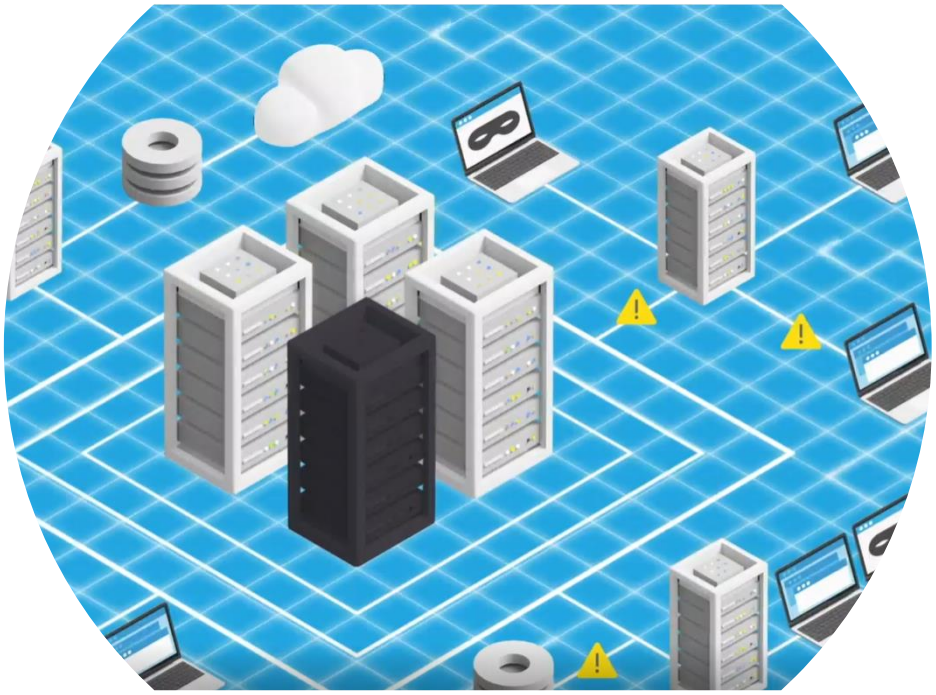
Automated Forensic Tool

Whitepaper

2022



National Technical University of Athens

Authored by:
Anna Georgiadou

ENERGY SHIELD

Automated Forensic Tool

IN A NUTSHELL

The **Automated Forensic Tool (AFT)** aims to extract information from external vulnerability databases to provide richer information for the investigation of security alerts detected by the EnergyShield SIEM tool.

The main purpose of the Automated Forensic tool is to assist in the investigation of cybersecurity incidents to have a deeper understanding of the context of the attack and the vulnerabilities that have been exploited. By linking and correlating indications of cyber-violations to information deriving from various security databases and knowledge bases, the Automated Forensic tool assists in better comprehending the possible tactics and techniques used by the adversaries to manipulate the existing IT and OT weaknesses while facilitating the forensic procedures.

> ***"AFT contributes to the classification, link and correlation between individual log entries/incidents and past events as presented in public, community-based databases of known vulnerabilities and related historical incidents.***
>
> *Anna Georgiadou, National Technical University of Athens*

CONTEXT

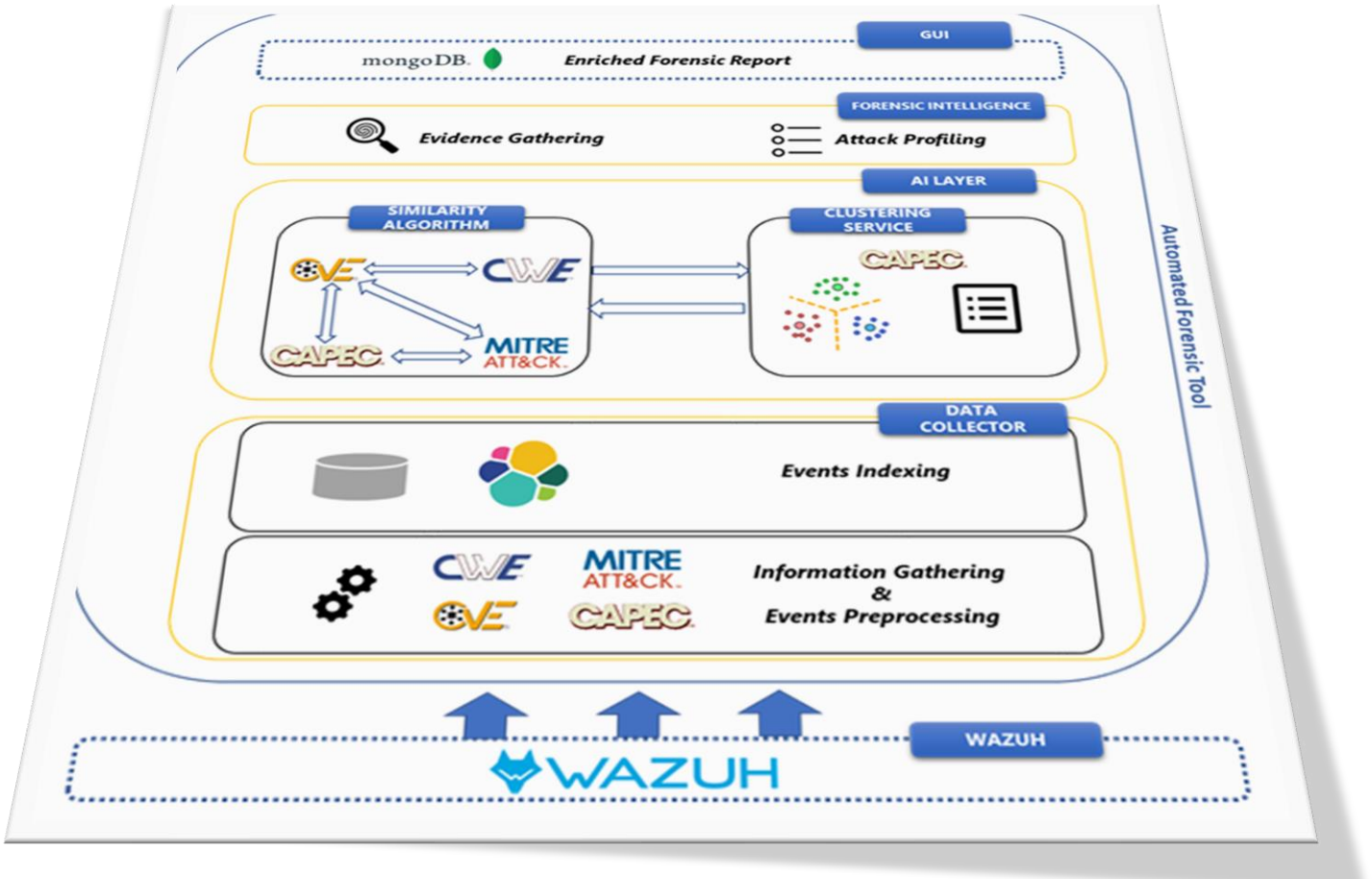
AFT generates a detailed digital report, along with its support evidence, that facilitates the investigation of security events detected by the rest of the EnergyShield modules and gathered by the SIEM tool. Its main objectives are to:

- facilitate the investigation of suspicious reported security events
- offer valuable insights on information related to privileges required, system specifications and misconfigurations
- identify exploited existing vulnerabilities, related attack patterns and adversary techniques
- conclude to alternative detection mechanisms and possible mitigation strategies

TECHNICAL DETAILS

The AFT is based on a modular architecture. Its main modules are:

- Data Collector: stores, indexes, and enriches data received from external and internal data sources.
- Artificial Intelligence (AI) Layer: consists of two subcomponents:
    - Similarity Algorithm: exploits text similarity and graph inference techniques.
    - Clustering Service: identifies similar entries creating clusters of related attack patterns and adversary techniques while generating a labelling mechanism.
- Forensic Intelligence Layer: gathers the information provided by the previous layers and combines it appropriately offering advanced profiling of the security breaches under investigation.
- Graphical User Interface (GUI): is responsible for presenting the elaborated forensic report to the end-users in an intuitive way facilitating security officers in the forensic investigation while offering different data visualisations and graphical representation capabilities.



ENERGYSHIELD DEMONSTRATOR

A SaaS version of the AFT has been made publicly available to both pilots of the EnergyShield project and to other interested parties, such as pilots from collaborating EU projects, scientific workshops, security agencies, etc.

EnergyShield pilot applications of the AFT tool:

- **Bulgarian Pilot:** The AFT tool was demonstrated to representatives of the Bulgarian pilot who subscribed to the SaaS version so as to familiarise themselves with and explore the capabilities of the tool.

  In a second phase, various actors in the Bulgarian energy value chain (TSO, DSO, generation plants, prosumer, etc.) were involved in a more detailed testing of the applicability and usability of the tool.

  A final piloting phase in a dedicated environment is currently taking place trimmed to the needs of the Bulgarian pilot.

**Due to the sensitive nature and special business needs the specific tool addresses, no further information can be publicly disclosed.*

BEST PRACTICES & LESSONS LEARNED

By combining information from different data sources and publicly available knowledge bases, the AFT identifies potential attacks and correlates them with vulnerabilities, detects attack patterns, and gathers evidence for adversary techniques. Similar security events noticed within the monitored network that might indicate an ongoing attack are also pinpointed, thus, supporting the forensic investigation and analysis. Most importantly, the AFT assists in the extraction of digital evidence and the interpretation of the recovered data while putting them in a logical and useful format. Thus, it leads to the preparation of a written report of findings which can, later on, be used for legal purposes.

Based on the EnergyShield piloting use cases, AFT's next steps include:

- further calibrating the tool for the specific needs of the pilots for the EPES sector;
- improving the classification and association links between the different sources as well as enhancing the mechanisms of creating these associations automatically through the use of deep learning techniques with lifelong learning capabilities;
- investigation of potential additional data sources and information to be used by the tool;
- evaluating and further improving the toolkit based on feedback provided by the pilots.

DISSEMINATION & COMMUNICATION

Articles presented in conferences:

- Touloumis, K., Michalitsi-Psarrou, A., Kapsalis, P., Georgiadou, A., & Askounis, D. (2021, December). Vulnerabilities Manager, a platform for linking vulnerability data sources. In 2021 IEEE International Conference on Big Data (Big Data) (pp. 2178-2184).

Dissemination **events**:

- SU-DS04-2018-2020 – Workshop: "Bridging three H2020 EU projects, EnergyShield, PHOENIX and SDN-microSENSE, all funded under the SU-DS04-2018-2020 programme and, consequently, sharing the same goals and vision towards Cybersecurity in the Electrical Power and Energy System (EPES)"
- CyberWatching - Webinar: "EPES and Smart GRIDS: practical tools and methods to fight against cyber and privacy attacks" (https://cyberwatching.eu/epes-and-smart-grids-practical-tools-and-methods-fight-against-cyber-and-privacy-attacks)
- EnergyShield – Workshop: "Present the trends, opportunities and choices in designing a cyber resilient EPES infrastructure"

ABOUT THE COMPANY

National Technical University of Athens (NTUA) is the most prestigious and most competitive academic institution for technical education in Greece. The Decision Support Systems Laboratory (DSSLab) is a multidisciplinary scientific unit within the School of Electrical and Computer Engineering, which conducts research and development, scientific / technical support and training activities addressing a wide range of complex research and application problems. Operating for more than 25 years, the lab has acquired international experience in the following sectors: Information Technology, Security and Decision Support Systems with a specialisation in e-Business and e-Government, Interoperability, Management Information Systems, Program & Project Management, Monitoring and Evaluation, Training and Human Resources Development, Information Dissemination and Promotion, Energy and Environmental Policy.

This project has received funding from the European Union's H2020 research and innovation programme under the Grant Agreement No. 832907

Website: www.energy-shield.eu **Twitter**: @EnergyShield_
LinkedIn Group; https://www.linkedin.com/groups/8831159/
Youtube channel: https://www.youtube.com/channel/UCtNRIf0uXvDsxVCSo1NfF_Q
E-mail: EnergyShield@siveco.ro