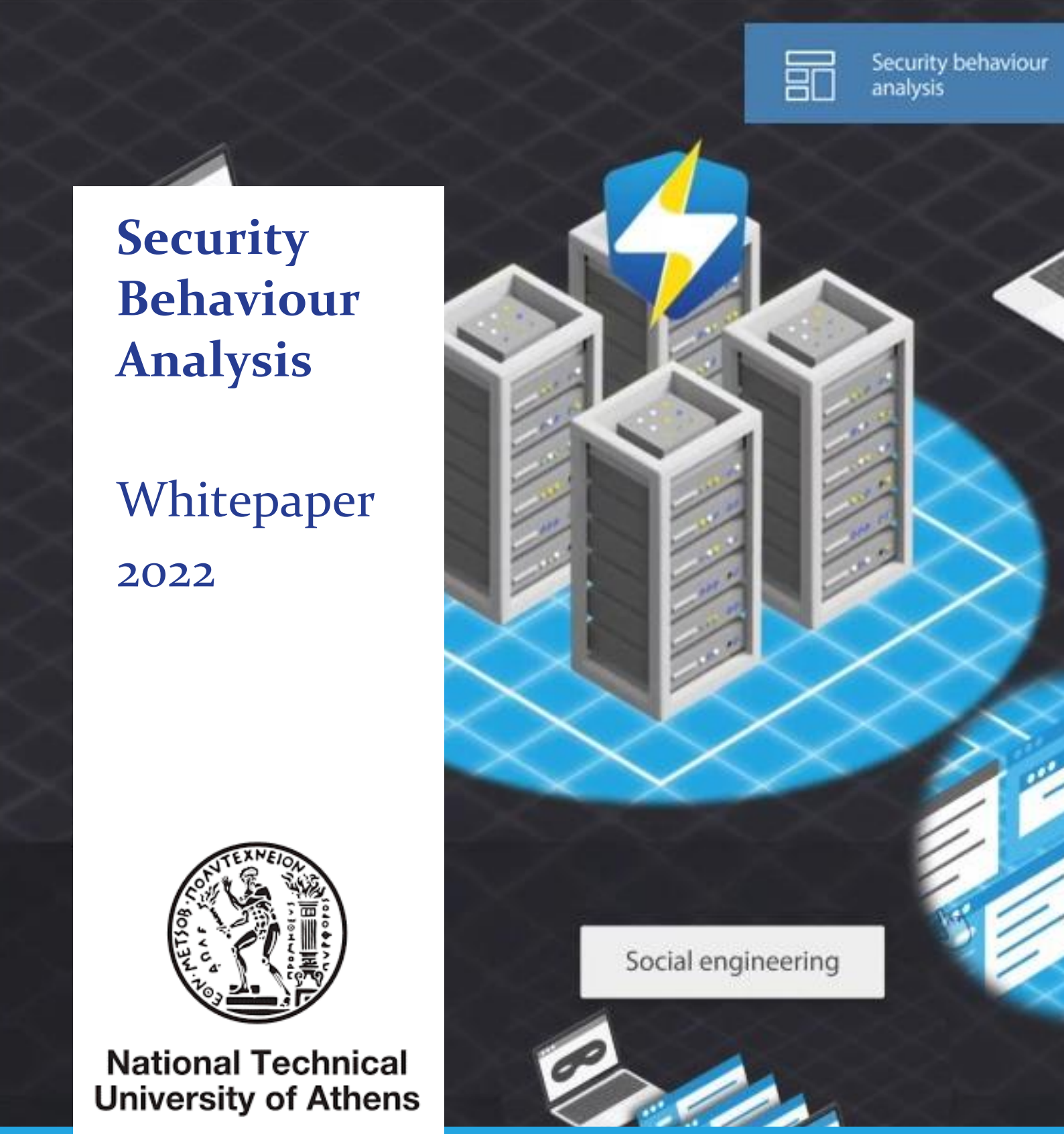
Security Behaviour Analysis

Whitepaper

2022



National Technical University of Athens

Authored by:
Anna Georgiadou

ENERGY SHIELD

Security Behaviour Analysis

IN A NUTSHELL

The **Security Behaviour Analysis (SBA)** tool aims to assess and map the socio-cultural behaviour of an organisation's workforce to cyberthreats. The tool is designed and implemented using a holistic approach to easily adapt and adjust to any business domain and, within the context of the project, it was adapted to and is being validated by the EPES sector.

SBA has been founded on **the Cyber-Security Culture (CSC)** framework. It is based on a combination of organisational and individual security factors structured into dimensions and domains. Its main goal is to examine organisational security policies and procedures in conjunction with employees' individual characteristics, behaviour, attitude, and skills. Each security metric introduced by the framework is assessed using a variety of evaluation techniques, such as surveys, tests, simulations, and serious games.

CONTEXT

The main purpose of the SBA tool is to assess and evaluate the current security readiness of an organisation's workforce. Its main objectives are to:

- perform the assessment of the security culture of an organisation at different levels (organisation, department units, employees, etc.);
- map the socio-cultural behaviour of end-users to specific cyber-threats;
- provide insights for decision-making regarding improving the security culture of the organisation;
- assist in planning and implementation of security culture training programs.

> ***"SBA bridges the professional with the scientific approach, the external with the internal indicators directly or indirectly related with cyber-security culture.***
>
> *Anna Georgiadou,*
> *National Technical University of Athens*

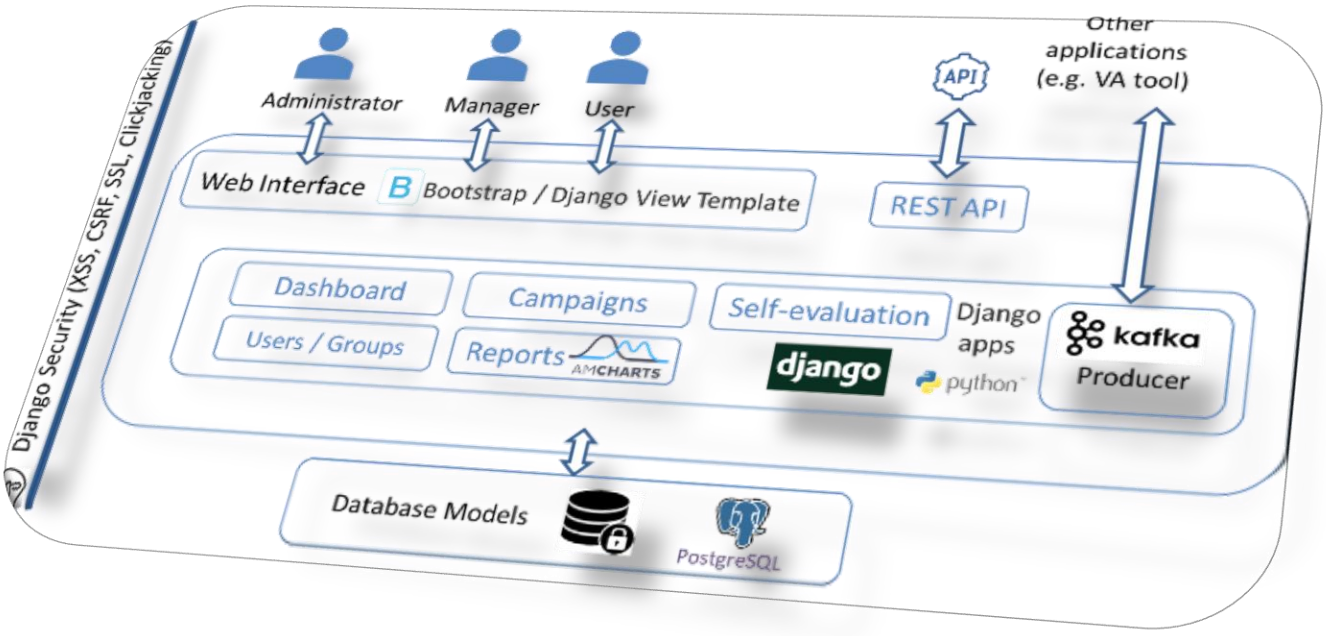
TECHNICAL DETAILS

SBA tool has been designed, developed, and implemented as a web application using a number of cut-edge technologies:

- **Django**: a high-level open-source Python Web framework;
- **PostgreSQL**: a powerful, open-source object-relational database system;
- **Web interface**: implemented using a combination of HTML, Bootstrap, CSS and JavaScript;
- **Kafka**: a producer publishing messages to specific Kafka topics to inform listening parties (Kafka consumers) that new evaluation data have become available (e.g., at the end of an assessment campaign).

SBA offers:

- sophisticated survey mechanism;
- assessment tests, simulations and serious games;
- results visualisation and reporting;
- assessment findings exposure;
- advanced user management and authentication;
- socio-cultural behaviour mapping to specific cyber-threats (MITRE ATT&CK & MERIT);
- decision-making insights;
- recommendations for security culture training programs;
- anonymisation;
- internationalisation and localisation.



ENERGYSHIELD DEMONSTRATOR

A SaaS version of the SBA tool (accessible at http://energyshield.epu.ntua.gr) 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 SBA tool:

- **Italian Pilot**: SBA tool was submitted to a significant cluster of beta-testers and early adopters who were selected to assess the business value and applicability of the questionnaires and games implemented. Each questionnaire of the SBA tool was analysed to evaluate its applicability to the specific use case scenario. In a second phase, the same analysis was carried out at a single-question level.

  Having concluded this testing phase, piloting was initiated in a dedicated integration environment where the Italian pilot has carefully designed an evaluation campaign targeting specific employee groups and practitioners to assess the overall company's cyber and physical security culture.

- **Bulgarian Pilot:** SBA 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. During this phase, specific roles were assigned to different partners so as to analyse in detail the possibilities offered via the assessment mechanism of the tool.

  A final piloting phase in a dedicated environment was concluded using different assessment techniques (questionnaires & simulations) trimmed to the needs of the Bulgarian pilot.

Other applications of the SBA tool:

- **Critical Infrastructures**: During the COVID-19 crisis, SBA was used to design a cyber-security culture assessment campaign targeting critical infrastructures. Its revealing findings provided significant feedback to the participating EU organisations. Insights and recommendations towards enforcing their cyber-security resilience were offered, further contributing to this research domain.
- **Health Domain**: SPHINX, an EU project aiming to enhance the cyber protection of the Health and Care IT Ecosystem, in collaboration with EnergyShield, designed, adjusted, and conducted a two-phase security awareness campaign targeting health sector personnel.

BEST PRACTICES & LESSONS LEARNED

The SBA tool has been designed and implemented to facilitate the assessment, cultivation, and improvement of the cyber-security culture status of an organisation via a holistic approach.

Numerous security elements and factors have been identified, listed, and grouped into different levels, dimensions, and domains, offering a hierarchical representation of the cyber-security readiness and overall reality of an organisation. Role segregation, key assessment concepts, and a specific evaluation methodology have been presented in detail, providing a useful guide through this rather demanding business procedure. Specific cyber-threats along with mitigation strategies, recommendations and targeted security awareness training programs are identified based on the assessment results achieved via the SBA tool.

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

- calibrating the security culture framework by adjusting the weights of each security element contained within the suggested model;
- evaluating and further improving both the suggested framework and tool based on the obtained feedback;
- fine-tuning the integration of SBA with the EnergyShield toolkit;
- expanding and adjusting our solution to other business domains and application areas;
- analysing the evaluation campaign results and publishing in scientific journals our findings from the EPES SBA applications.

DISSEMINATION & COMMUNICATION

Articles in scientific journals:

- Georgiadou, A., Mouzakitis, S., Bounas, K. & Askounis, D. (2020) A Cyber-Security Culture Framework for Assessing Organization Readiness, Journal of Computer Information Systems
- Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Designing a cyber-security culture assessment survey targeting critical infrastructures during COVID-19 crisis. International Journal of Network Security & Its Applications (IJNSA) Vol, 13 (1).
- Georgiadou, A., Mouzakitis, S. & Askounis, D. Working from home during COVID-19 crisis: a cyber security culture assessment survey. Security Journal (2021).

- Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Detecting Insider Threat via a Cyber-Security Culture Framework. Journal of Computer Information Systems, 1-11.
- Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Assessing MITRE ATT&CK risk using a Cyber-Security Culture Framework. Sensors, 21(9), 3267.
- Georgiadou, A., Michalitsi-Psarrou, A., Gioulekas, F., Stamatiadis, E., Tzikas, A., Gounaris, K., Doukas G., Ntanos C., Landeiro Ribeiro L. & Askounis D. (2021, October). Hospitals' Cybersecurity Culture during the COVID-19 Crisis. In Healthcare (Vol. 9, No. 10, p. 1335). Multidisciplinary Digital Publishing Institute.
- Gioulekas, F., Stamatiadis, E., Tzikas, A., Gounaris, K., Georgiadou, A., Michalitsi-Psarrou, A., Doukas G., Kontoulis M., Nikoloudakis Y., Marin S., Cabecinha R. & Ntanos, C. (2022, February). A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures. In Healthcare (Vol. 10, No. 2, p. 327). MDPI.

Articles presented in **conferences**:

- K. Bounas, A. Georgiadou, M. Kontoulis, S. Mouzakitis, D. Askounis (2020), Towards a CyberSecurity Culture Tool Though a Holistic, Multi-Dimensional Assessment Framework, 13th IADIS International Conference Information Systems 2020, p.135-139, Sofia, 2020. ISBN: 978-989-8704-15-3
- Georgiadou, A., Mouzakitis, S., & Askounis, D. (2020). Towards Assessing Critical Infrastructures Cyber-Security Culture During Covid-19 Crisis: A Tailor-Made Survey. arXiv preprint arXiv:2012.13718
- Hacks, S., Butun, I., Lagerström, R., Buhaiu, A., Georgiadou, A., & Michalitsi Psarrou, A. (2021, August). Integrating Security Behaviour into Attack Simulations. In The 16th International Conference on Availability, Reliability and Security (pp. 1-13).

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