PROJECT

Multitenant Cybersecurity Operations Centre Delivered as an Open Cloud Service with Machine Learning Capabilities

V29 Final Project Report

KPB9 – final report

type – report

delivery month – M24

Funded by the European Union
NextGenerationEU

RECOVERY AND RESILIENCE PLAN

GOVERNMENT OFFICE OF THE SLOVAK REPUBLIC

Contents

1. Executive Summary 3
2. Summary of Objectives Achieved within the Defined Period 3
3. Summary of Deliverables Submitted within the Defined Period 4
4. Summary of Key Events and Risks 6
5. Key Lessons Learnt and Recommendations for Future Development 7

1. EXECUTIVE SUMMARY

The final report was prepared for month M24, marking the final completion of the project. It was prepared jointly by the project managers of both partners (FRI, BRAIN:IT). It comprises five main sections, and the supporting material for its preparation was submitted by the leaders of all work packages.

The aim of the project was to design and implement a security operations centre as a cloud service that uses multitenancy principles and machine learning capabilities to improve the detection of and response to cyber threats.

The report summarises the deliverables and progress achieved between **April 2024 (M1) and March 2026 (M24).** It documents 29 deliverables in detail, including analyses, component designs, criteria, the logical framework, the technological architecture and monitoring mechanisms.

2. SUMMARY OF OBJECTIVES ACHIEVED WITHIN THE DEFINED PERIOD

The main objective of the project was to design an open, multitenant security operations centre (SOC) solution to be provided as a cloud/container service with scalable processing capacity and modules for anomaly detection and prediction using machine learning and neural networks. To ensure the achievement of the main project objective, five **specific project objectives** were identified:

1. Design of a technological solution for operating the SOC service using virtualised solutions, developed to TRL3.
2. Design of an intelligent system for monitoring technological resources and services.
3. Design of the architecture of the innovative elastic INNOSOC service itself through the integration of open solutions and components.
4. Design of suitable machine learning algorithms using deep neural networks to address the detection and prediction of security and operational anomalies.
5. Creation of a platform for sharing the knowledge acquired in the project in accordance with the principles of open science.

The specific objectives were achieved by carrying out activities within the work packages linked to the respective objectives. The achievement of all specific objectives led to the achievement of the overall project objective. The design of the multitenant security operations centre (SOC) solution was completed.

The achievement of the objectives also depended on the production and delivery of the specified deliverables (V1-V29). The submission of some deliverables was postponed for justified reasons, but this did not affect the achievement of the objectives by the end of the project. The revised submission dates for the affected deliverables are recorded in the following section (Table 1).

3. SUMMARY OF DELIVERABLES SUBMITTED WITHIN THE DEFINED PERIOD

Table 1 lists the deliverables for the period M1-M24, together with their planned and actual delivery dates. These were summarised on the basis of deliverable *V25 Project Schedule* and *V28 Interim Project Report*. Subsequent progress was then monitored and assessed at the end of month M24 during the preparation of this final report.

Table 1 Deliverables for the specified period

Deliverable No.	Deliverable	Work package code	Entity responsible for the deliverable	Type	Verification method	Planned delivery (project month)	Actual delivery (project month)
V1	results of the analysis of available solutions	KPB1	UNIZAFRI	documentation	complete documentation	M3 (Jun 24)	M3 (Jun 24)
V2	list of defined criteria	KPB1	UNIZAFRI	list	approved list	M5 (Aug 24)	M5 (Aug 24)
V3	description of the selected solution meeting the specified criteria	KPB1	UNIZAFRI	documentation	complete documentation	M7 (Oct 24)	M7 (Oct 24)
V4	results of the analysis of suitable components	KPB2	UNIZAFRI	documentation	complete documentation	M3 (Jun 24)	M3 (Jun 24)
V5	list of defined criteria	KPB2	UNIZAFRI	list	approved list	M5 (Aug 24)	M5 (Aug 24)
V6	description of dashboards and the monitoring and reporting system	KPB2	UNIZAFRI	documentation	complete documentation	M7 (Oct 24)	M7 (Oct 24)
V7	results of the analysis of suitable algorithms	KPB3	UNIZAFRI	documentation	complete documentation	M10 (Jan 25)	M18 (Sept 25)*
V8	list of defined criteria	KPB3	UNIZAFRI	list	approved list	M10 (Jan 25)	M18 (Sept 25)*
V9	description of the selected algorithm meeting the specified criteria	KPB3	UNIZAFRI	documentation	complete documentation	M17 (Aug 25)	M18 (Sept 25)*
V10	list of functional and non-functional requirements	KPB4	BRAIN:IT	list	approved list	M14 (May 25)	M14 (May 25)
V11	business architecture	KPB4	BRAIN:IT	documentation	approved documentation	M16 (Jul 25)	M16 (Jul 25)
V12	technological architecture	KPB4	BRAIN:IT	documentation	approved documentation	M19 (Oct 25)	M19 (Oct 25)
V13	DNR – detailed solution design with annexes	KPB4	BRAIN:IT	documentation	complete documentation	M22 (Jan 26)	M22 (Jan 26)
V14	operational infrastructure	KPB5	BRAIN:IT	documentation	operational infrastructure	M19 (Oct 25)	M22 (Jan 26)**
V15	software components	KPB5	BRAIN:IT	list	approved list	M20 (Nov 25)	M22 (Jan 26)**
V16	functional PoC	KPB5	BRAIN:IT	documentation	stable, functional cloud service	M22 (Jan 26)	M22 (Jan 26)

V17	test results and evaluation	KPB5	BRAIN:IT	test protocol	approved test protocol	M24 (Mar 26)	M24 (Mar 26)

Deliverable No.	Deliverable	Work package code	Entity responsible for the deliverable	Type	Verification method	Planned delivery (project month)	Actual delivery (project month)
V18	published indexed journal articles	KPB6	UNIZAFRI	articles	library registration, indexing	M24 (Mar 26)	M24 (Mar 26)
V19	conference papers included in proceedings	KPB6	UNIZAFRI	proceedings	library registration, indexing	M24 (Mar 26)	M24 (Mar 26)
V20	creation of an online platform	KPB7	BRAIN:IT	information portal	online availability	M15 (Jun 25)	M15 (Jun 25)
V21	awareness-raising materials and outputs available online	KPB7	BRAIN:IT	educational materials	approved list	M22 (Jan 26)	M22 (Jan 26)
V22	awareness-raising activities undertaken	KPB7	BRAIN:IT	activities	list of participants, photographic documentation	M24 (Mar 26)	M24 (Mar 26)
V23	updated project justification	KPB8	UNIZAFRI	documentation	approved by the Project Board	M3 (Jun 24)	M3 (Jun 24)
V24	updated project logical framework	KPB8	UNIZAFRI	documentation	approved by the Project Board	M3 (Jun 24)	M3 (Jun 24)
V25	updated tools for monitoring the project schedule and achievement of objectives	KPB8	UNIZAFRI	documentation	approved by the Project Board	M5 (Aug 24)	M5 (Aug 24)
V26	updated expenditure against the allocated budget	KPB8	UNIZAFRI	documentation	approved by the Project Board	M6 (Sept 24)	M6 (Sept 24)
V27	risk register	KPB8	UNIZAFRI	register	approved by the Project Board	M3 (Jun 24)	M3 (Jun 24)
V28	interim project report	KPB8	UNIZAFRI	report	approved by the Project Board	M12 (Mar 25)	M12 (Mar 25)
V29	final project report	KPB9	UNIZAFRI	report	approved by the Project Board	M24 (Mar 26)	M24 (Mar 26)

**The capacity of project team members was overstretched, resulting in the postponement of the previously scheduled deadlines for deliverables V7, V8 and V9. A mitigation measure was applied: sharing the impacts among the partners involved in the project. The finalisation of deliverables V7, V8 and V9 was postponed to month M18. Partner BRAIN:IT provided additional capacity to assist with deliverables V7 and V8.*

***The selected technologies did not meet all the relevant defined requirements during the final review before proceeding to the next step, owing to a change in the commercial status of the "The Hive" component. The final submission deadline for deliverables V14 and V15 had to be postponed to month M22. A new component was selected, on the basis of which deliverables V14 and V15 were revised.*

4. SUMMARY OF KEY EVENTS AND RISKS

The initial risks were identified by month M3 as part of deliverable **V27 Risk Register** (KPB8). These were further developed by month M12, when the interim report (V28) was prepared. An addendum to deliverable V27 was therefore created, entitled **Supporting Material for V28_Updated Risk Register as at Month M12.** This was updated as required throughout the project until M24. Triggering events (triggers) were identified in the risk register. The leader of the relevant work package was responsible for monitoring them.

Several issues arose during the project and were detected on the basis of the defined triggering events recorded in the risk register. The most significant risks included R7, R9 and R15.

R7 – Failure to monitor project bottlenecks. Trigger: A bottleneck arose that had not been identified in advance. This involved overstretched capacity among project team members, resulting in the postponement of the previously scheduled deadlines for deliverables V7, V8 and V9. The same risk later also affected the delivery of V11 and V12.

R9 – Communication inconsistencies between partners. Trigger: Communication noise occurred, and project team members involved in the activities repeatedly requested information that had already been provided.

R15 – Errors in the supporting material for the updated project justification. Trigger: An error was detected when the project manager accepted the deliverable at milestone MS1 (further information in the Milestones section).

R19 – Incorrect selection of technologies for the SOC system. Trigger: The selected technologies did not meet all the relevant defined requirements during the final review before proceeding to the next step. The materialisation of this risk was associated with a change in the commercial status of the “The Hive” component. The final submission deadline for deliverables V14 and V15 had to be postponed to month M22.

R25 – Difficulties in coordinating team members during the summer months (M16, M17) owing to annual leave taken by the project team.

5. KEY LESSONS LEARNT AND RECOMMENDATIONS FOR FUTURE DEVELOPMENT

The project confirmed the importance of continuously monitoring and updating risks throughout implementation. It demonstrated that recording risks in a register is an important foundation, but that the ability to identify their actual occurrence promptly, assess their impact on the schedule and take appropriate action without delay is equally essential. The experience gained during the project also highlighted several areas that provide important lessons for future development.

Risk R7 confirmed the need to monitor capacity bottlenecks more rigorously and identify overstretched team members in good time. Failure to recognise this situation adequately led to delays in several deliverables. An important recommendation is therefore to review capacity regularly at work package level, share the impacts among partners promptly and provide scope for flexibly increasing staffing capacity according to current needs.

Risk R9 demonstrated that communication inconsistencies can arise even when shared communication tools are used, reducing the efficiency of collaboration. An important lesson is therefore the need to establish clearer communication rules, preferred tools and the frequency of coordination meetings at an earlier stage of the project. It is also advisable to check regularly whether the chosen communication arrangements meet the actual needs of the partners involved.

Risk R15 highlighted the need to strengthen internal quality control of deliverables before their official submission. The detection of errors only at the point of acceptance confirmed the importance of more rigorous internal verification of supporting material. It is therefore recommended that more systematic control mechanisms be introduced in future to help reduce errors and ensure smoother achievement of milestones.

Risk R19 confirmed that the suitability of technological solutions needs to be reviewed continuously during project implementation, as well as at the initial selection stage. The change in the commercial status of the “The Hive” component demonstrated that external factors can significantly affect the implementation of planned activities. Future work should therefore emphasise rigorous definition of criteria, ongoing verification of the sustainability of the selected solutions and preparedness for alternative technological options.

Risk R25 confirmed that even predictable periods, such as summer holidays, can significantly affect team coordination. Important recommendations therefore include planning absences in advance, sharing this information transparently and adapting coordination arrangements to periods of reduced team availability.

Recommendations for Further Technical Development of the Solution

In addition to organisational and project management lessons, the project also identified key areas for the further development of the proposed SOCaaS solution.

Key directions for further development include closer integration between the individual architectural layers, particularly the SIEM, SOAR, CTI and incident management components. The degree of interconnection between them is proving to be a decisive factor in the overall effectiveness of the solution, particularly in terms of incident processing speed, contextual enrichment of events and consistency of response procedures. Another important area is the

development of processes and staffing arrangements for SOC operations. The project experience demonstrated that the technological architecture must be accompanied by clearly defined roles, responsibilities, communication links and team capacity planning. Without an appropriate process and organisational framework, stable and efficient operation of the proposed solution cannot be ensured in the long term.

We consider the detailed development of an approach to separating data, access rights, incident workflows and operational contexts between individual tenants to be an outstanding technical challenge requiring closer attention, so that the functional, security and operational aspects of service provision are all maintained. A higher degree of automation is another important direction for further development. The project confirmed the benefits of automated integration and response mechanisms, with further development focusing primarily on extending playbooks, automating incident enrichment and reducing the proportion of manual steps in repeatable SOC analyst activities.

Another area identified is the extension of testing to a wider range of scenarios and more realistic operating conditions. Further validation should address not only the functionality of individual components but also the robustness of integration flows, the response to more complex incident scenarios and the stability of the solution under higher volumes of data and events. Finally, the use of machine learning methods for anomaly detection and decision support in the SOC environment remains a promising area for future development. Further advances in this area could contribute to more accurate identification of selected incident types, better event classification and more efficient processing of larger data streams.

Overall, the project generated important insights not only into capacity management, communication, deliverable control and technological decision-making, but also into the design and validation of the architecture of a multitenant SOCaaS solution. The experience gained provides a sound basis for organising similar projects more effectively and for further technical development of the proposed solution.