Addressing the challenge
Illicit activities on the Dark Web are more than just a challenge for law enforcement agencies: each year, individuals in the US lose more than USD 1.4 billion to internet fraud. Globally, the cost of data breaches from cyber-attacks hit USD 2.1 trillion in 2019 – over four times the estimated cost four years earlier. Businesses are further impacted by the establishment of black markets, such as for counterfeit products or prescription drugs. As business-specific knowledge is often required to combat these issues, situational awareness of cyber-crime is a must.

Proposed solutions
Although various monitoring and detection tools already exist, their effectiveness is reduced by a lack of interoperability. The DEFRAUDify (Detect Fraudulent Activities in dark web and clear web to protect your business) project will therefore enhance functionalities with automated, proactive monitoring that can generate business-specific threat analyses. A Fraud Intelligence Suite will then combine these tools in a flexible, interoperable manner in order to support visualisation and historical replays. A particular innovation is the deployment of autonomous software agents which use active monitoring to uncover the most relevant intelligence information. Other emphases include privacy by design and quantifiable results to support boardroom decision-making. Three use-cases will demonstrate this: cryptocurrency fraud detection; strategic risk monitoring; and unusual financial transaction assessment.

Projected results and impact
DEFRAUDify’s most important outcome is the reduction of fraud-related costs via the identification of criminal activities, allowing businesses to prepare against them. In terms of efficiency, for instance, the project expects to reduce the detection time for cryptocurrency scams from four hours to ten minutes, allowing businesses to act before large damage can be inflicted. As for coverage, DEFRAUDify’s trend identification tool should be able to uncover more online communities or activities which are potentially harmful for a specific business than currently is possible. This has the additional benefit of increasing end-user trust in digital services and cyber-security. Exploitation can be carried out independently by all business partners, but joint exploitation will yield additional power in the global fraud detection and prevention market, expected to reach USD 29.07 billion by 2023 at a 16.42% compound annual growth rate. DEFRAUDify therefore anticipates over USD one million in sales growth for participating commercial companies. The intended standardisation of the interoperability-by-design approach and cyber-risk evaluation will only serve to expand the market potential of this project.
ITEA is the Eureka R&D&I Cluster on software innovation, enabling a large international community of large industry, SMEs, start-ups, academia and customer organisations, to collaborate in funded projects that turn innovative ideas into new businesses, jobs, economic growth and benefits for society. ITEA is part of the Eureka Clusters Programme (ECP).

https://itea4.org