EDF-2022-RA-CYBER-CSACE: Adapting cyber situational awareness for evolving computing environments

Budget

The Union is considering a contribution of up to EUR 10 000 000 for this topic under the call EDF-2022-RA

Number of actions to be funded: Several actions, addressing different solutions, may be funded for this topic

Objectives

General objective

An increasing number of malicious actions targeting governmental and strategic systems occur in cyber space. New or improved solutions, technologies and applications for enhanced cyber situational awareness (CSA) are essential to counter these threats. To address evolving and more complicated activities in cyberspace, including challenges that arise due to the ongoing evolution of battlefield network and systems, decision makers and Security Operation Centre (SOC) operators need the most updated CSA related to cyber threats, in real time, gathering internal and external cyber information. CSA denotes the capability for a decision-maker to know what is going on in the cyber domain in order to be able to make informed decisions and adequately respond to incidents.

Specific objective

CSA needs to be supported by technology to collect, correlate and fuse the several sources of data as well as their different nature (e.g., network, mission, open-source intelligence, structured and unstructured threat awareness) to provide the necessary information so that human decision-makers can assimilate the situation. Cyber threats continue to grow in complexity and scope, new and evolving threats arising from advancing adversary campaigns and tactics and at the same time the volume and diversity of cyber threat intelligence grows all the time. It poses challenges to human operators to visualise and comprehend the variety and volumes of information produced by dynamic and fragmented networks and systems in a battlefield context. The evolving computing challenges will require improved mission awareness capabilities through Cyber Threat Intelligence (CTI) establishing interfaces with

sources of information considered relevant for the planning and conduct phases of an operation in order to provide real time mission information at the correct level of granularity to the common operational picture (COP).

Scope and types of activities

Scope

The overall goal is to explore novel concepts and operational opportunities for providing to the Commander essential intelligence about the adversary, their capabilities and objectives while operating in and through cyberspace. CTI enhanced with a Semantic Threat Enrichment module able to analyse both data coming from public repositories and the dark web to generate Indicators of Compromise (IoCs) and Indicators of Attacks (IoAs) will support Cyberspace Operations.
The proposals are expected to develop novel solutions leveraging full-spectrum cyber defence (physical, logical, cyber persona) under an adversarial-focused perspective. The proposals are

expected to aim at CSA-supporting technology with a view to provide the necessary technical information elements that are needed to process the vast amounts of information in order to produce from tactical to COPs, as well as other technical artifacts to be used by decision- makers in need of CSA. This includes creation of graphics like timelines, histograms or relationship graphs, personalized dashboards, and reports according to the responsibilities of each user. Special attention shall be paid to the interoperability and collaboration with existing solutions at Security Operations Centre (SOC), Network Operations Centre (NOC) and Computer Emergency Response Team (CERT) level, where duplication of effort is to be avoided.
The proposals are expected to cover state of the art technologies. Enhanced situational awareness information handling and visualisation systems are expected to have a capability to present overarching views of the battlefield environment through COPs via data exportable modules of logic information to be interoperable with other operational pictures be at land, sea, air or space, taking into account ongoing evolution of the C2 military systems towards the Internet of the Military Things (IOMT) scenario which poses additional complexity, and sustain against a massive attack to critical battlefield system.

Types of activities

The following types of activities are eligible for this topic:

Types of activities (art 10(3) EDF Regulation)		Eligible?
(a)	Activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence (**generating knowledge**)	Yes (optiona
(b)	Activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies (**integrating knowledge**)	Yes (optiona
(c)	**Studies**, such as feasibility studies to explore the feasibility of new or upgraded products, technologies, processes, services and solutions	Yes (mandatory
(d)	**Design** of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such design has been developed, including partial tests for risk reduction in an industrial or representative environment	Yes (mandatory
(e)	**System prototyping** of a defence product, tangible or intangible component or technology	No
(f)	**Testing** of a defence product, tangible or intangible component or technology	No
(g)	**Qualification** of a defence product, tangible or intangible component or technology	No

Types of activities (art 10(3) EDF Regulation)		Eligible'
(h)	**Certification** of a defence product, tangible or intangible component or technology	No
(i)	Development of technologies or assets **increasing efficiency** across the life cycle of defence products and technologies	No

The proposals must include studies and design. The proposal may include generating knowledge and integrating knowledge activities.

The following tasks must be performed as part of the required activities:

1. Development of a number of typical user scenarios based on stakeholder needs. Entails analysis of battlefield IOMT technology requirement and their impact on the collection, correlation and presentation of information. It will include advances in terms of organisational, leadership and human training capability aspects. These will take into consideration human-machine interphases and performance optimisation in e.g., cyber SOCs.

2. The use of the digital twin concept and human factors analysis to improve operator information acquisition and processing through enhancing the current COP artefact technologies. Digital twins can allow to overcome operational technology (OT) constraints due to the need to be continuously operational and the fact they often provide only limited in-depth analysis capabilities. Digital twins can run in parallel to their physical counterparts and allow inspection of their behaviour without the risk of disrupting operational services.

3. Development of different hierarchical models to support IOMT mission awareness. These should establish means of aggregating dependency information to propagate only mission relevant, abstracted information rather than entire network configurations. Moreover, these systems must be able to exchange dependency information between and across federated IoT systems from different organisations/trust domains.

4. Design of an AI multi-stage (i.e., multi kill chain steps) attack detection architecture that maps AI-based anomaly detection models onto the distributed enterprise infrastructure. This will enable efficient temporal and spatial correlations of the event streams from different endpoints. This is expected to exceed the performance of conventional centralized security systems through improved detection of cross- network attacks and greatly reduced data communication. Moreover, it is essential to integrate threat modelling and sharing with attack detection to achieve efficient real-tie detection using AI.

5. The use of federated learning to create a collaborative intrusion detection system (CIDS) to enhance the inter-domain sharing of mission-oriented CTI as well as remove many of the trust and privacy issues associated with CTI sharing. In this approach no actual alerts are shared, rather the AI model parameters are shared. This will ensure that there is no leakage of sensitive network, organisational or personal information. Moreover, the CIDS pattern can be implemented within a single organisation through judicious partitioning.

6. The use of digital ledger technologies to facilitate more dynamic and incentivised mission-oriented CTI sharing analysis between organisations well as increasing trust in sharing of intrusion model parameters between cross-domain federated learning entities will be investigated.
7. The following tasks may be performed as part of the eligible activities:
8. linking observed tactics and techniques to specific Advanced Persistent Threat (APT) behaviour, which may assist with adversary characterization and identification;
9. use of deception technologies, including decoys, both for monitoring the threat landscape and attackers' behaviour, and for intrusion detection. Particular attention should be on making the data from such systems can be presented in useful ways, and integrated with other sources of information;
10. use of machine learning technology.
11. The proposals must substantiate synergies and complementarity and avoiding unnecessary duplication with projects awarded under EDIDP calls for proposals.

Functional requirements

Proposals should meet the following functional requirements:

- Definition of a number of use-case scenarios to test the concept.
- Development of proof-of-concept implementations to verify the operation.
- Design of a cyber-range-based environment simulation to both generate representative data sets to validate the AI models and to provide a testbed to evaluate the overall concept.

Expected impact

The outcome is expected to contribute to:

- Better understanding of how CTI along with future technology will be able to support an analyst's build-up and conservation of a high level of CSA.
- Improved visualisation metaphors and information handling processes arising from IOMT scenarios.
- Improved CSA management through simulation capabilities provided by digital twins.
- Improved mission-to-asset awareness for IOMT supported mission infrastructures.
- Increased CTI sharing due to use of federated learning to prevent leakage or need to share sensitive information.
- Better understanding on the use of distributed anomaly detection in both single organisation constituencies as well as the effectiveness of collaborative intrusions on improving attack detection.