Cyber MAR

Cyber-MAR Final and Piraeus Pilot Event

The Prediction Engine

Giorgos Drainakis & Markos Antonopoulos, ICCS

16th December 2022

Overarching Idea of the engine

- The ICCS Prediction Engine in Cyber-MAR aims at:
  - **Systematically model past knowledge** on attack behavior patterns
  - **Provide real-time predictions** concerning vulnerable parts of the infrastructure.
  - **Facilitate educated decisions** based on **past knowledge** and **possible risks and/or economic impacts** during an ongoing cyberattack.
- For each simulated attack scenario, the engine receives, processes and fuses information from:
  - IDS sensors
  - XL-SIEM output events
  - Risk models
  - Econometric models

Event and Event Sequence Modeling

- What the engine will perceive as an **event** is defined as a triplet of

(Event_type, Source_subnetwork, Dest_subnetwork)

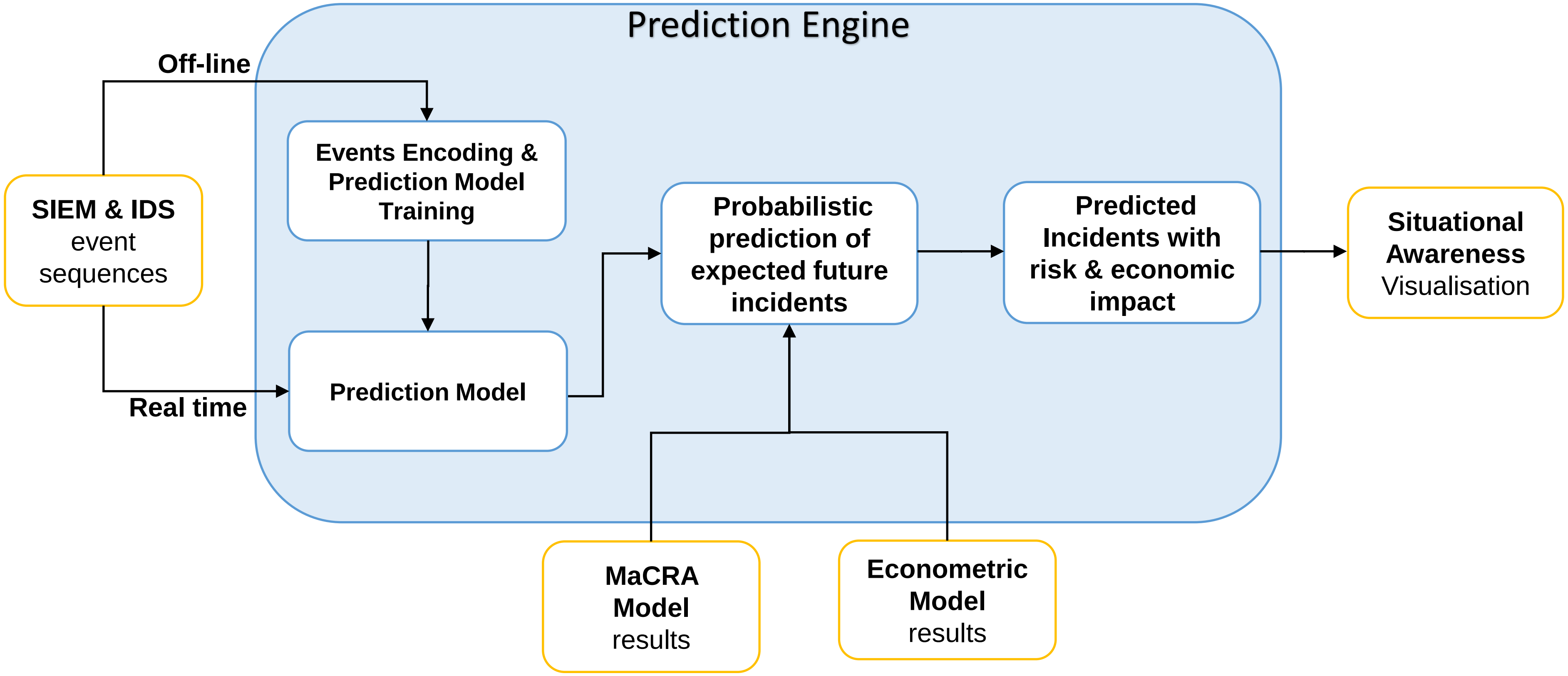
Where:

- **Event_type** is either the alert type of the corresponding IDS alert or the SID_NAME of the corresponding SIEM event.
- **Source_subnetwork**, **Dest_subnetwork** may be any relevant subnetwork of the infrastructure.

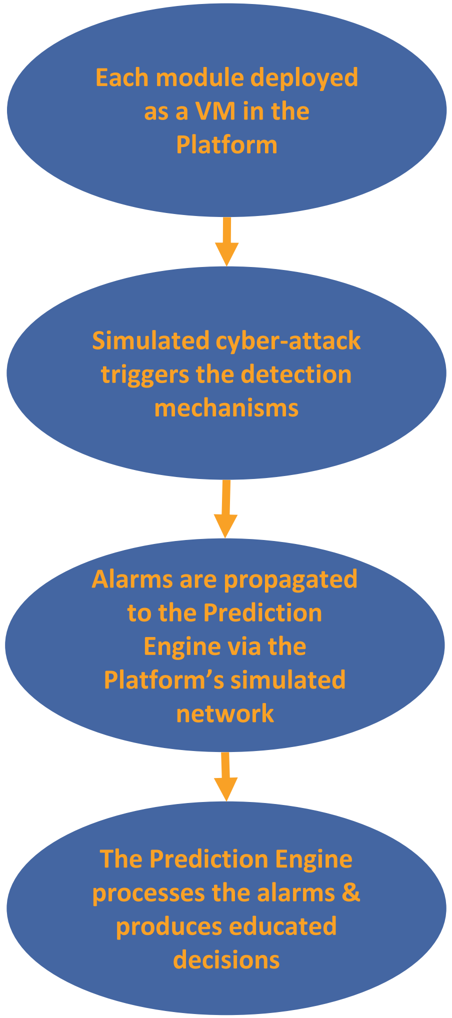
- Each **event** is matched to a **code word**, i.e. a string of characters. This essentially encodes a **sequence of events** into a **sequence of strings**.

- Sequences of strings are then modeled by a Variable Length Markov Model, implemented by a properly extended Suffix Tree data structure.

Probabilistic Prediction Engine Logic


Prediction Engine
Off-line
SIEM & IDS event sequences
Events Encoding & Prediction Model Training
Real time
Prediction Model
Probabilistic prediction of expected future incidents
Predicted Incidents with risk & economic impact
Situational Awareness Visualisation
MaCRA Model results
Econometric Model results

Pilot 3 Topology & Deployment

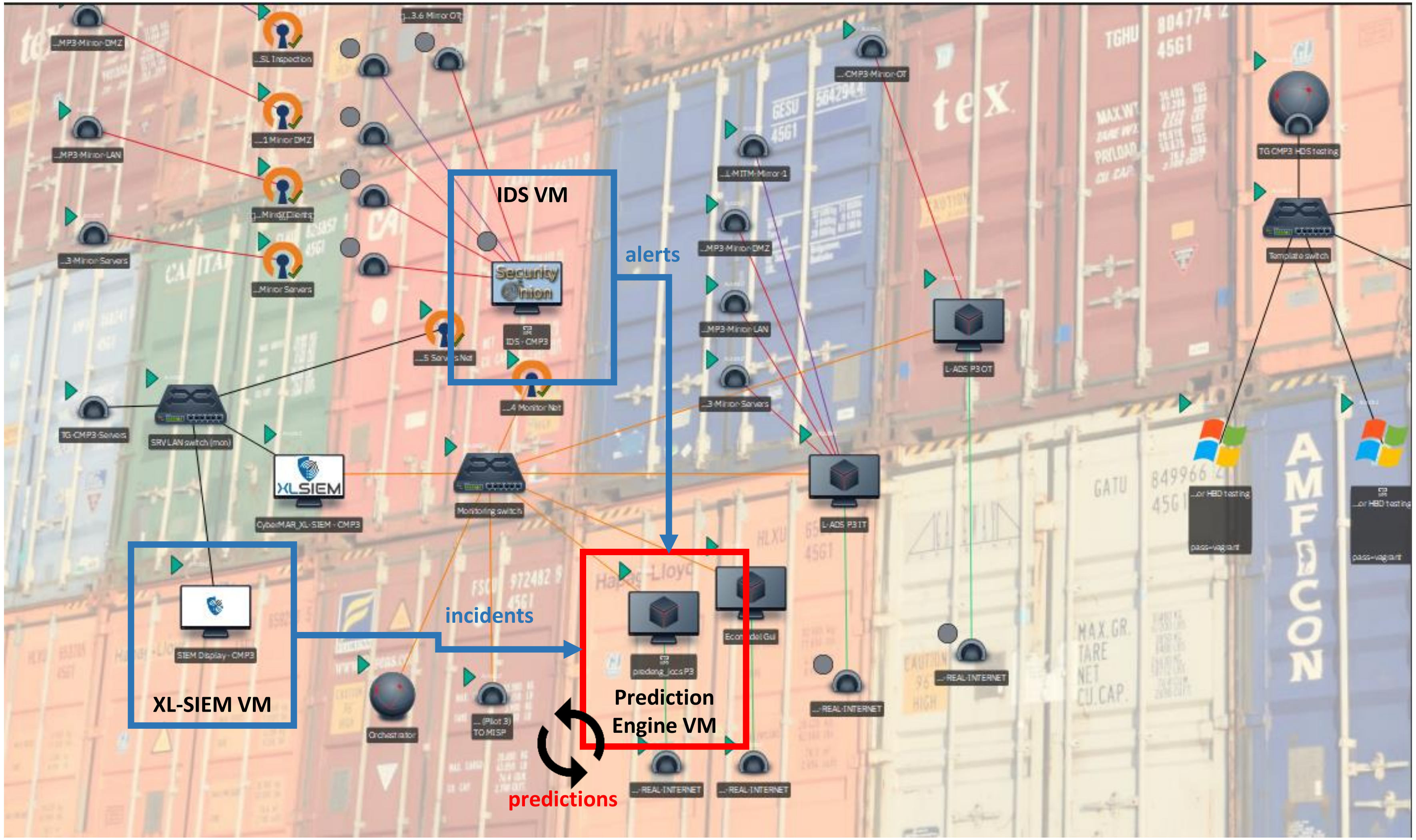


Each module deployed as a VM in the Platform

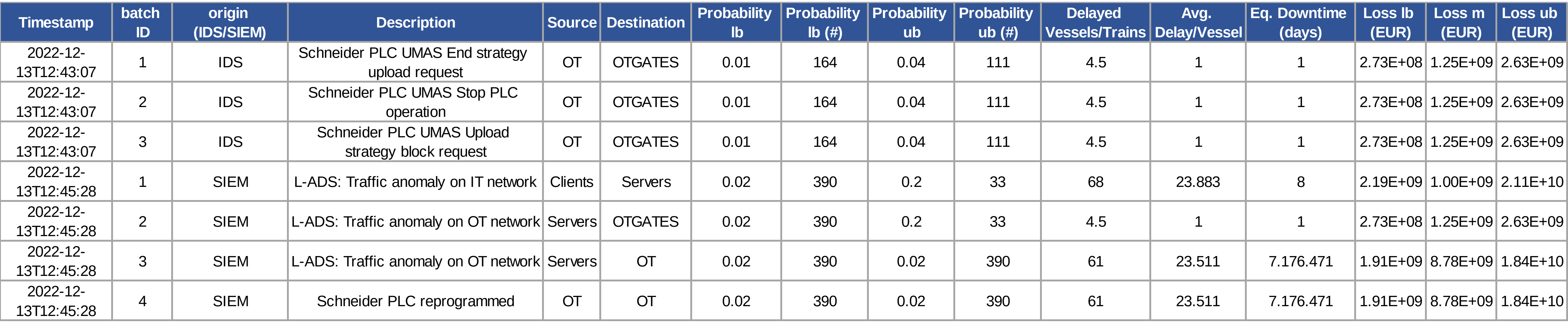
Simulated cyber-attack triggers the detection mechanisms

Alarms are propagated to the Prediction Engine via the Platform's simulated network

The Prediction Engine processes the alarms & produces educated decisions



Exemplary output

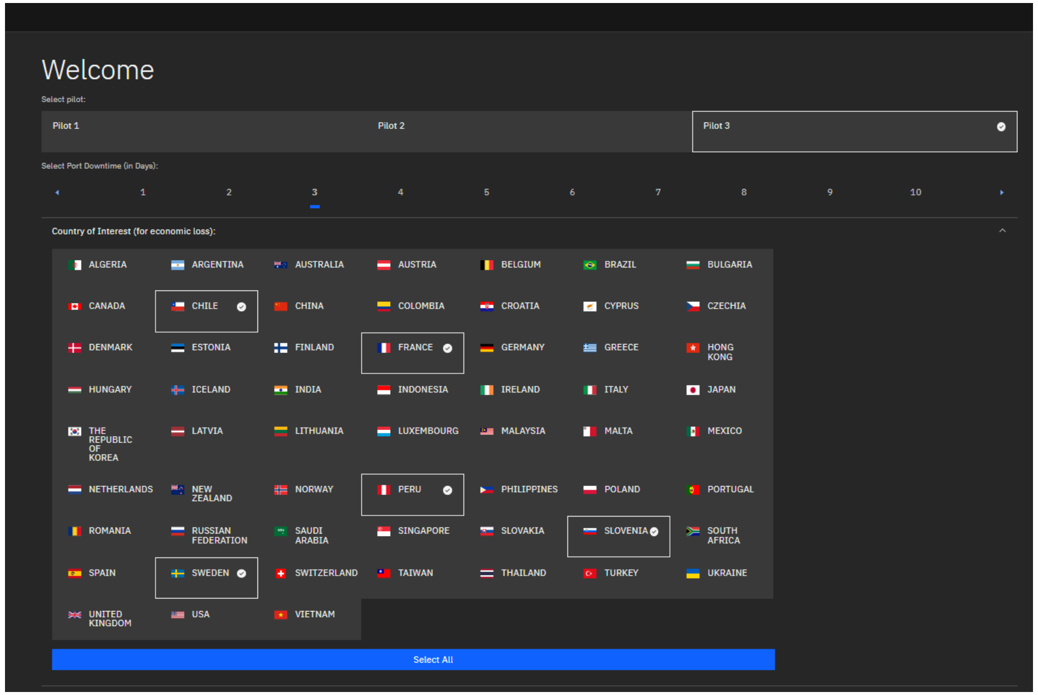


Timestamp	batch ID	origin (IDS/SIEM)	Description	Source	Destination	Probability lb	Probability lb (#)	Probability ub	Probability ub (#)	Delayed Vessels/Trains	Avg. Delay/Vessel	Eq. Downtime (days)	Loss lb (EUR)	Loss m (EUR)	Loss ub (EUR)
2022-12-13T12:43:07	1	IDS	Schneider PLC UMAS End strategy upload request	OT	OTGATES	0.01	164	0.04	111	4.5	1	1	2.73E+08	1.25E+09	2.63E+09
2022-12-13T12:43:07	2	IDS	Schneider PLC UMAS Stop PLC operation	OT	OTGATES	0.01	164	0.04	111	4.5	1	1	2.73E+08	1.25E+09	2.63E+09
2022-12-13T12:43:07	3	IDS	Schneider PLC UMAS Upload strategy block request	OT	OTGATES	0.01	164	0.04	111	4.5	1	1	2.73E+08	1.25E+09	2.63E+09
2022-12-13T12:45:28	1	SIEM	L-ADS: Traffic anomaly on IT network	Clients	Servers	0.02	390	0.2	33	68	23.883	8	2.19E+09	1.00E+09	2.11E+10
2022-12-13T12:45:28	2	SIEM	L-ADS: Traffic anomaly on OT network	Servers	OTGATES	0.02	390	0.2	33	4.5	1	1	2.73E+08	1.25E+09	2.63E+09
2022-12-13T12:45:28	3	SIEM	L-ADS: Traffic anomaly on OT network	Servers	OT	0.02	390	0.02	390	61	23.511	7.176.471	1.91E+09	8.78E+09	1.84E+10
2022-12-13T12:45:28	4	SIEM	Schneider PLC reprogrammed	OT	OT	0.02	390	0.02	390	61	23.511	7.176.471	1.91E+09	8.78E+09	1.84E+10

Abbreviations: lb, lower bound
m, mean value
ub, upper bound
#, number of samples for probability estimation

Econometric Model App

- Econometric model (EM) service: A web-app to explore the results of the Prediction Engine
- Separate Web UI for each predicted event
- Allows the user to explore the economic impact of various attack scenarios and configurations



Welcome

Select pilot:

Pilot 1 | Pilot 2 | Pilot 3 ✓

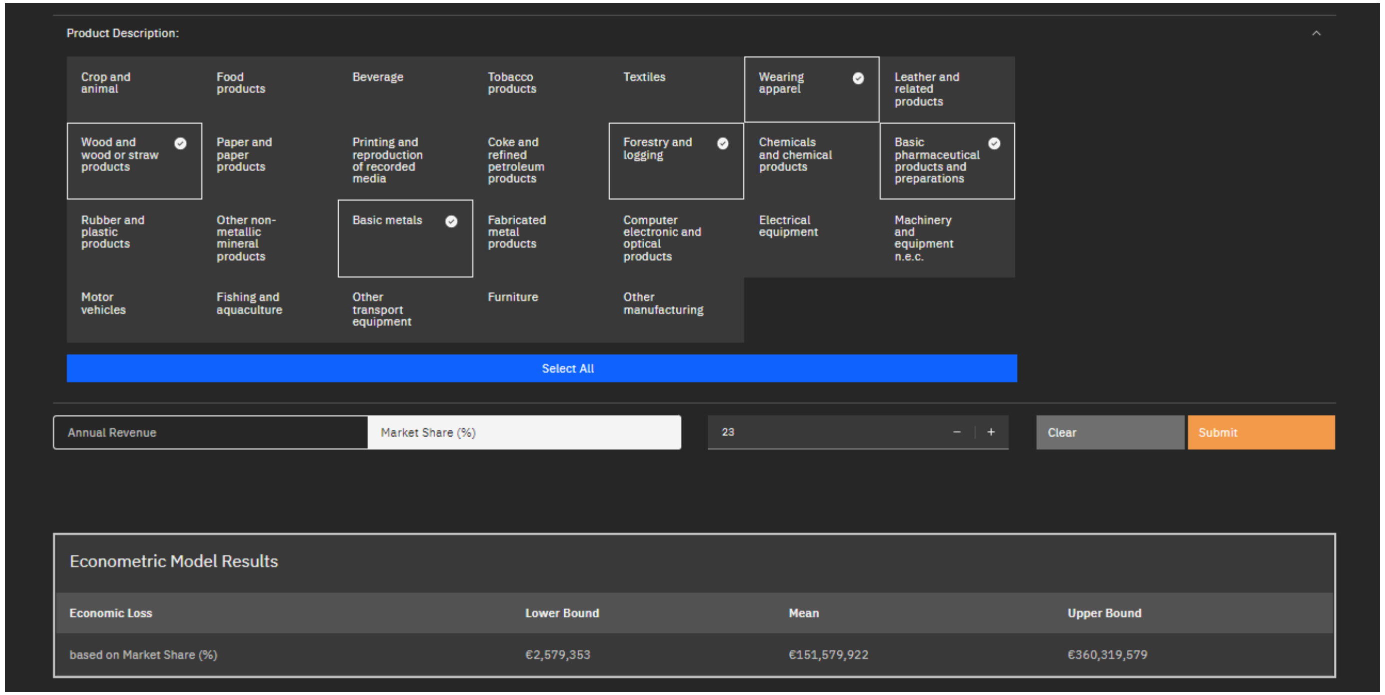
Select Port Downtime (in Days):

◂ 1 2 **3** 4 5 6 7 8 9 10 ▸

Country of Interest (for economic loss):

ALGERIA	ARGENTINA	AUSTRALIA	AUSTRIA	BELGIUM	BRAZIL	BULGARIA
CANADA	CHILE ✓	CHINA	COLOMBIA	CROATIA	CYPRUS	CZECHIA
DENMARK	ESTONIA	FINLAND	FRANCE ✓	GERMANY	GREECE	HONG KONG
HUNGARY	ICELAND	INDIA	INDONESIA	IRELAND	ITALY	JAPAN
THE REPUBLIC OF KOREA	LATVIA	LITHUANIA	LUXEMBOURG	MALAYSIA	MALTA	MEXICO
NETHERLANDS	NEW ZEALAND	NORWAY	PERU ✓	PHILIPPINES	POLAND	PORTUGAL
ROMANIA	RUSSIAN FEDERATION	SAUDI ARABIA	SINGAPORE	SLOVAKIA	SLOVENIA ✓	SOUTH AFRICA
SPAIN	SWEDEN ✓	SWITZERLAND	TAIWAN	THAILAND	TURKEY	UKRAINE
UNITED KINGDOM	USA	VIETNAM				

Step1. User selects source port (pilot), downtime and country of interest



Product Description:

Crop and animal	Food products	Beverage	Tobacco products	Textiles	Wearing apparel ✓	Leather and related products
Wood and wood or straw products ✓	Paper and paper products	Printing and reproduction of recorded media	Coke and refined petroleum products	Forestry and logging ✓	Chemicals and chemical products	Basic pharmaceutical products and preparations ✓
Rubber and plastic products	Other non-metallic mineral products	Basic metals ✓	Fabricated metal products	Computer electronic and optical products	Electrical equipment	Machinery and equipment n.e.c.
Motor vehicles	Fishing and aquaculture	Other transport equipment	Furniture	Other manufacturing		

Annual Revenue | Market Share (%) | 23 − +

Econometric Model Results

Economic Loss	Lower Bound	Mean	Upper Bound
based on Market Share (%)	€2,579,353	€151,579,922	€360,319,579

Step2. User selects products of interests and market share/revenues and collects the predicted econometric losses

www.Cyber-MAR.eu

Cyber_MAR

Cyber-MAR EU Project

Cyber-MAR

info@lists.Cyber-MAR.eu

THANK YOU FOR YOUR ATTENTION

Giorgos Drainakis ICCS
Markos Antonopoulos ICCS

✉ giorgos.drainakis@iccs.gr
markos.antonopoulos@iccs.gr

This project has received funding from the European Union’s horizon 2020 research and innovation programme under grant agreement No. 833389