2022 IEEE CSR
Workshop on Cyber Ranges and Security Training

Design and proof of concept of a prediction engine for decision support during cyber range attack simulations in the maritime domain

Markos Antonopoulos, Giorgos Drainakis, Eletherios Ouzounoglou,
Giorgos Papavassiliou, Angelos Amditis, ICCS

28 July 2022

Infrastructure Network Security

- Network technologies are adopted in almost all contemporary infrastructures.
- Network technologies are ever-growing in complexity.
- Cyber threats are ever-evolving in sophistication.
- Testing and evaluation of such systems from a cybersecurity perspective poses significant challenges.
- Both a standardized technology plus a methodology for systematically analysing and effectively facing cyber attacks remain elusive.

Cyber Ranges

- Cyber Ranges are an emerging technology promising to provide solutions to the aforementioned challenges.
- Cyber Ranges are interactive and/or simulated representations of events of an organization's local network, system, tools and applications.
- Cyber Ranges enable comprehensive simulation and testing of the network under consideration, including elements like actual or simulated devices, virtual machines, software, webpages plus a variety of potential cyber attacks.
- Thus, they provide a virtual but realistic playground for:
  - **Continuous training** of cyber security experts.
  - **Design** and **testing** of tools and methods aiming to aid the defender.

Overarching Idea of the Prediction Engine

- In this work, we leverage the simulating capabilities of cyber range technology to design a tool aiming to serve as a decision support system (called the Prediction Engine) for maritime cyber security personnel during an ongoing simulated cyber attack.
- The engine is designed to **receive**, **process** and **fuse** information from:
  - Intrusion Detection System (IDS) sensors.
  - Security Information and Event Management (SIEM) output events.
  - Risk estimations (inflicted delays and downtime).
- Aiming to:
  - Systematically model **past knowledge** on attack behavior patterns.
  - Provide **real-time predictions** concerning vulnerable parts of the infrastructure.
  - Provide an additional tool facilitating **educated decisions** based on past knowledge and possible risks and/or economic impacts during an ongoing cyber attack.

Network Attack Modeling Approaches for Threat Prediction

Attack Graphs - main idea: Utilize alert correlation to create attack models (i.e. graphs depicting attack steps), use them to make predictions

- Attack Graphs-rule based:
  - Aiming to “provide an efficient representation and algorithmic tools to identify the possible cases system vulnerabilities can be exploited in a network”
  - Rely on a comprehensive and accurate knowledge of the system vulnerabilities
- Attack Graphs-probability based:
  - Map sensor (IDS/SIEM) observable events to high level attack patterns using Bayesian Networks
  - High level attack patterns need to be pre-defined by domain experts. How many? How much detail ? How to update them?
- Modeling Attacker behavior e.g. in terms of Capability, Intent, Opportunity etc.
  - Still quite immature to provide robust models

Prediction by learning Attack Patterns

- Detailed information on network vulnerabilities and high level attack strategies cannot easily be obtained nor maintained/updated.
- Several works have focused on learning attack patterns without relying on detailed network knowledge and a priori defined attack behaviors.
- The Variable-Length Markov model (VLMM) forms a concrete example of such approaches. Given a discrete set E of possible events, an attack is modeled by an ordered finite sequence {e_i }_(i=1)^N. A VLMM considers all n-th order Markov models, i.e. the probabilities

$$P_n\{X_{t+1} = e | X_t = e_0, \dots, X_{t-(n-1)} = e_{n-1}\} \text{ where } e_i \in E \; \forall \; i = 0, \dots, n-1, n \geq 1$$

  - Training a VLMM requires simply event sequences from past attacks
  - Enables the discovery and combination of patterns within attack sequences
  - Has been shown to display good performance on predicting next attack steps

Modeling – definitions

- In terms of the event logs provided by the IDS and SIEM modules, a **cybersecurity event** is a large and complex structure of information regarding a large variety of features of what can be defined as a cybersecurity event. These features include source and destination IPs, ports and protocols, type of event among many others.
- The core notion of the entire approach is the notion of a **cybersecurity incident**, or simply **incident**, which essentially models a subset of the information describing a cybersecurity event.
- From a modeling perspective, the notion of what we will consider as an incident is something to be defined by modeling decisions.
  - It is impractical to include all the aforementioned information in the definition of the incident notion. It would be difficult to detect and model patterns in a sequence of such rich and complex structures.
  - Plus, it would most certainly require vast amounts of data.
- Thus, what the engine will perceive as an **incident** is a modeling decision and is to be defined according to what practical purpose it is planned to serve, plus the availability of pertinent data.

Modeling – examples

- Useful alternative definitions of what the engine will perceive as an **incident** may be the following:
  - a triplet of (IDS_event_type, Source_IP, Dest_IP), where
    - IDS_event_type is an IDS indication e.g. dns, fileinfo, flow, http, alert etc.
  - a triplet of (SIEM_event_type, Source_IP, Dest_IP), where
    - SIEM_event_type is an SIEM indication e.g. malware, zerologon attack, modicon quantum attack etc.
- A more generic model of an **incident** may also be the following, which takes into account subnetworks rather that specific IPs.
  - a triplet of (SIEM_event_type, Source_subnetwork, Dest_subnetwork), where
    - SIEM_event_type is an SIEM indication as above and Source_subnetwork, Dest_subnetwork may be OT_network, Servers_LAN, Users_LAN, DMZ etc.
- The approach is general enough to enable consideration of a wide variety of possible definitions of the notion of an **incident**; apart from IDS and/or SIEM event-based definitions, any type of discrete event concerning the port infrastructure may by included and/or combined with others.

Incident encoding and the Suffix Tree representation of past knowledge

- Once the notion of an **incident** has been defined in a useful and practical way, each **incident** will be matched to a **code word**, i.e. a string of characters.
  - This enables the encoding of a **sequence of incidents** into a **sequence of strings**.
- The entire set of complete attack sequence can then be represented compactly in a Suffix Tree structure, properly extended to handle sequences of strings instead of sequences of single characters
- Such a representation models the knowledge that can be extracted in terms of **attack behavior patterns** consisting of **incident (string) sub-sequences** observed in the entire set of **complete incident (string) sequences** obtained by simulated cyber-attack scenarios.
- Apart from a compact representation, the Suffix Tree structure consists a complete and computationally efficient* implementation of a VLMM.

  **searching for a pattern is O(n), where n is the length of the pattern.*

Modeling example (SIEM data)

Incident model and encoding

Abbreviations: SLAN, Servers LAN
ULAN, Users LAN
OT, Operational Technology (PLCs)

Incident Encoding

a: DMZ_to_SLAN/Policy violation, DNS update from external server detected on DST_IP

b: SLAN_to_SLAN/Policy violation, DNS update from external server detected on DST_IP

c: ULAN_to_SLAN/Policy violation, DNS update from external server detected on DST_IP

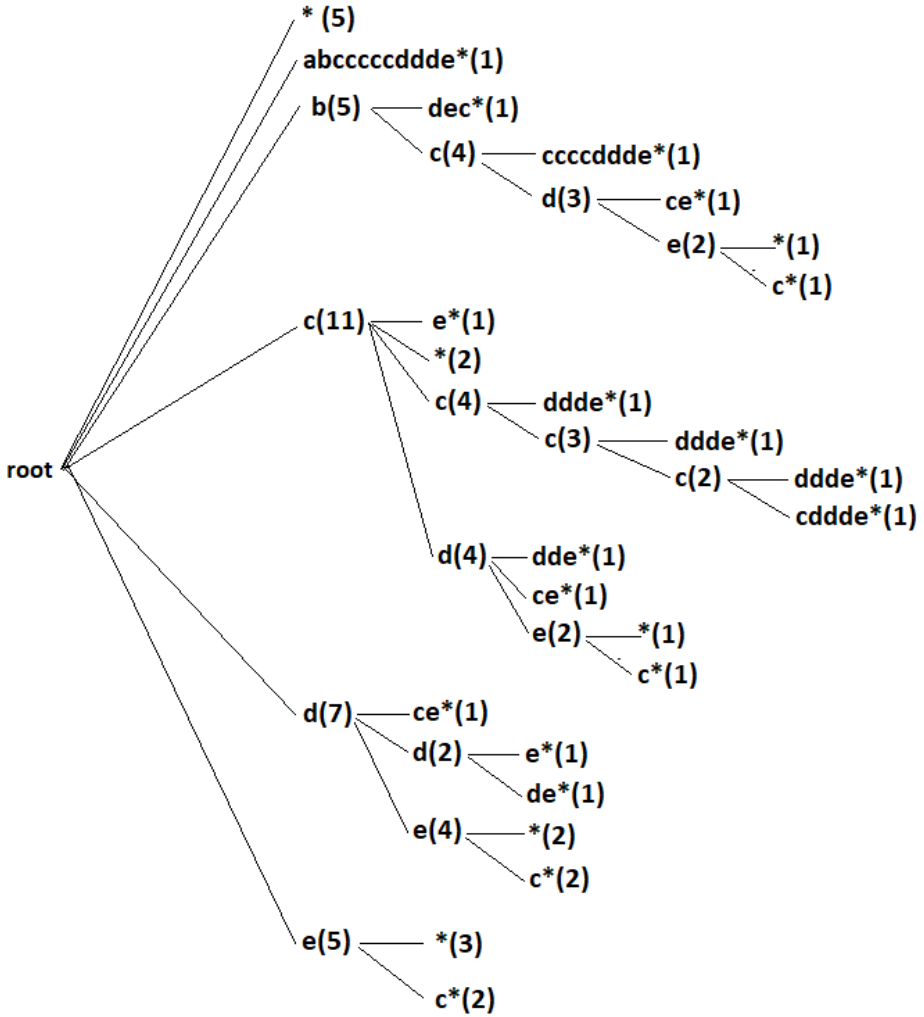
d: ULAN_to_SLAN/Zerologon Attack detected - CVE-2020-1472

e: OT_to_OT/Modicon Quantum attack attempt

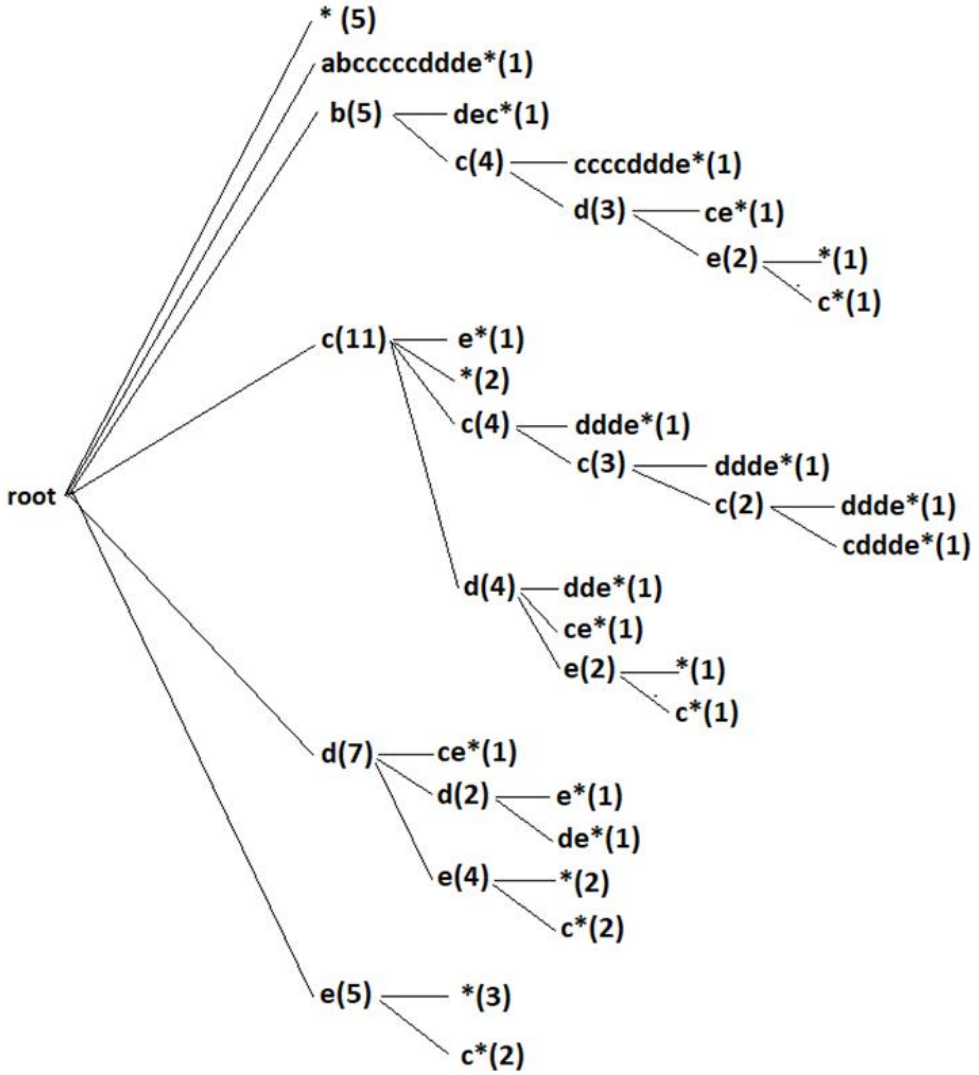
Incident (alarm) Sequences from XL-SIEM from 5 simulated attacks *(* denotes end of sequence)*:

a-b-c-c-c-c-c-d-d-d-e-*
b-c-d-e-*
b-d-e-c-*
b-c-d-c-e-*
b-c-d-e-c-*

Suffix Tree



Single Step Inference (next event)



Input sequence : **a-b-c**
query: **What's next ?**

pattern	#occurences	a	b	c	d	e	*
a-b-c	1			1			
b-c	4			1	3		
c	11			4	4	1	2

Next event	Probability(#samples)
a	0%
b	0%
c	36% (11) - 100% (1)
d	36% (11) – 75% (4)
e	9% (11)

a : DMZ_to_SLAN/Policy violation, DNS update from external server detected on DST_IP

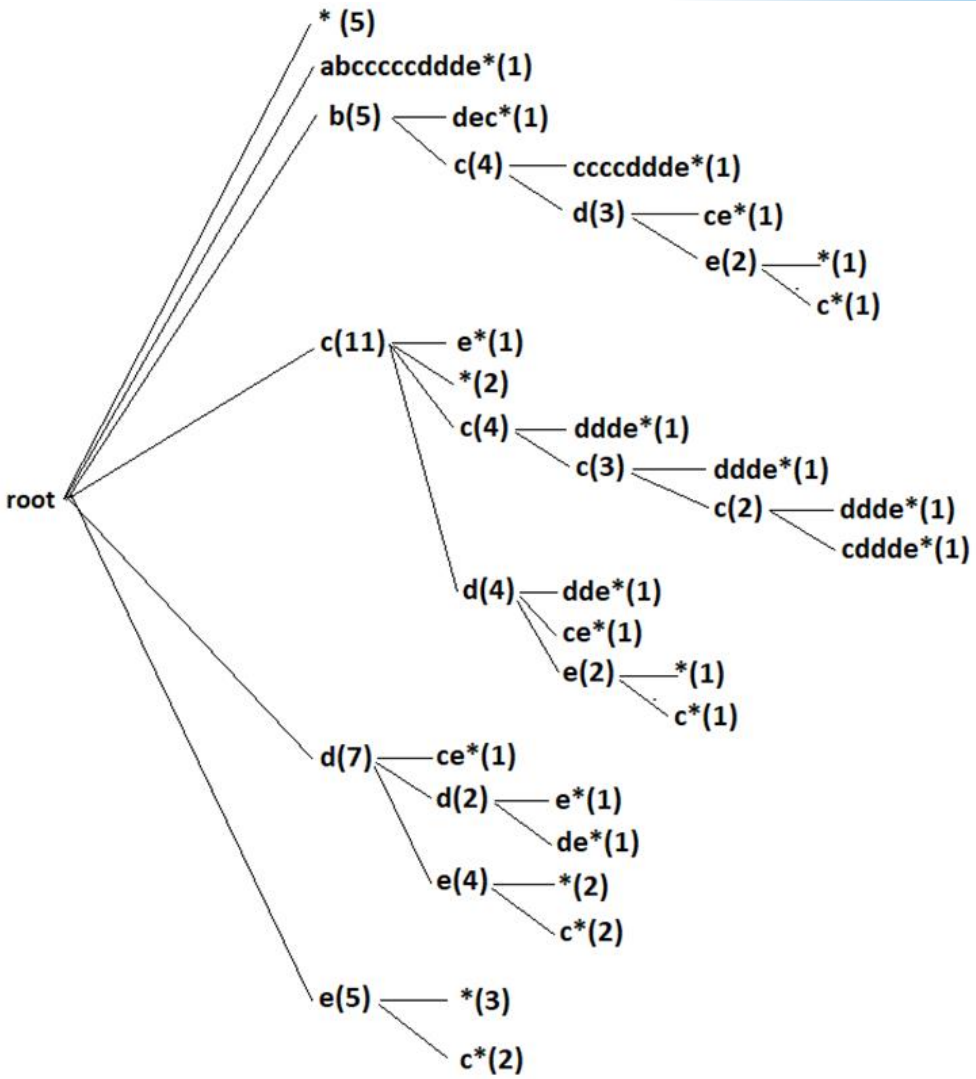
b : SLAN_to_SLAN/Policy violation, DNS update from external server detected on DST_IP

c : ULAN_to_SLAN/Policy violation, DNS update from external server detected on DST_IP

d : ULAN_to_SLAN/Zerologon Attack detected - CVE-2020-1472

e : OT_to_OT/Modicon Quantum attack attempt

Multistep Inference



Input sequence : **a-b-c**

query: **What is the probability of observing event *x* in the next *n* events? (here *x* = e, *n* = 3)**

pattern	Probability(#samples)
a-b-c	0% (1)
b-c	75%(4)
c	36%(11)

Estimated probability: 36%(11) – 75%(4)

a: DMZ_to_SLAN/Policy violation, DNS update from external server detected on DST_IP

b: SLAN_to_SLAN/Policy violation, DNS update from external server detected on DST_IP

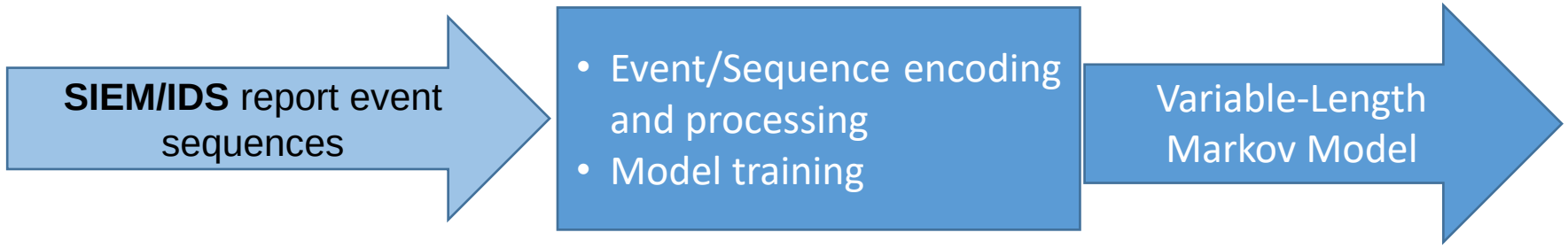
c: ULAN_to_SLAN/Policy violation, DNS update from external server detected on DST_IP

d: ULAN_to_SLAN/Zerologon Attack detected - CVE-2020-1472

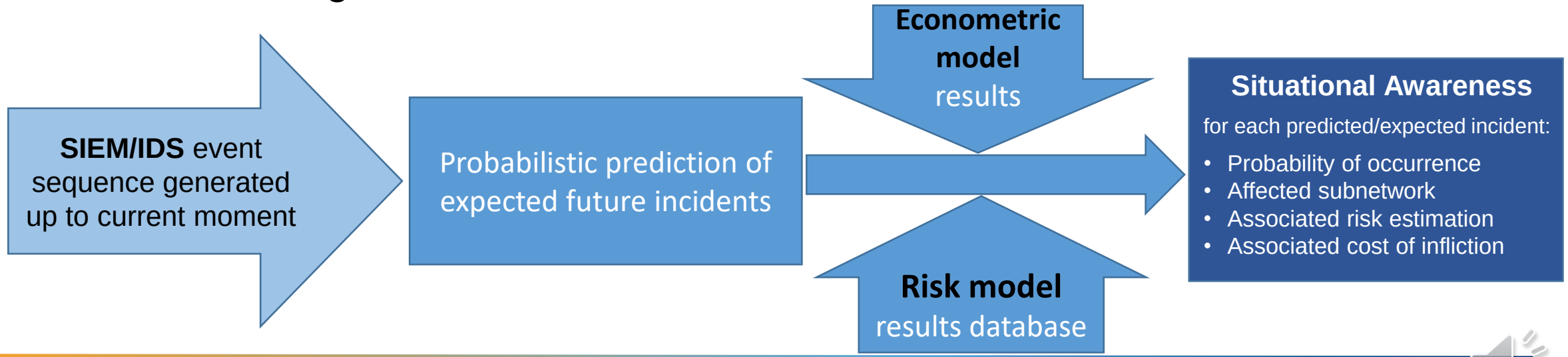
e: OT_to_OT/Modicon Quantum attack attempt

The Prediction Engine Logic

Off-Line Modelling:

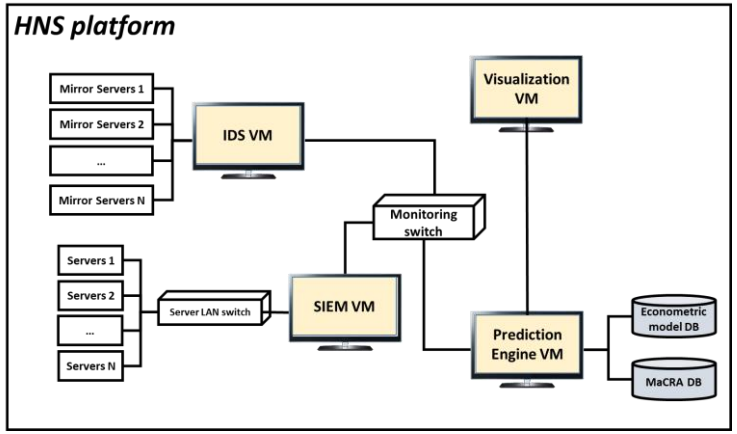


On-line Predicting:



Technical Details

- Integration in Cyber-MAR
  - Module instantiation via Virtual Machines (VMs)
  - Hybrid Network Simulation (HNS) cyber range
    - VM management
    - Network simulation
    - Cyber attack simulation
  - Interfaces with other modules
    - **IDS** for alert monitoring (via syslog)
    - **SIEM** for incident monitoring (via RabbitMQ)
    - **MaCRA** for port disruption modeling (static database)
    - **Visualization** module for output/predictions presentation (via syslog)
- Future Work
  - Integration of **Econometric Model**
    - A user-configurable database, attached to the Prediction Engine
    - Risk estimation & evaluation of associated cost of a cyber attack
  - Testing & Deployment
    - System-wise & functionality tests in the HNS platform
    - Cyber-attack scenario in port of Piraeus (Oct/Nov 2022)



Prediction Engine integration into HNS platform, an actual cyber range

3-DigitNAICS	3-DigitTrade	MeanEconomicLossIndex	LBEconomicLossIndex	UBEconomicLossIndex
999	100000	0,6	0,48	0,72
998	100001	0,34	0,27	0,41
997	100002	0,02	0,02	0,02
996	100003	0,1	0,08	0,12
995	100004	0,65	0,52	0,78
994	100005	0,92	0,74	1,1
993	100006	0,52	0,42	0,62
992	100007	0,64	0,51	0,77

Econometric Model: Testing data schema

Exemplary output

Timestamp	batch ID	origin (IDS/SIEM)	Description	Source	Destination	Probability lb	Probability lb(#)	Probability ub	Probability ub(#)	Delayed Vessels	Avg. Delay/Vessel (days)	Eq. Downtime (days)
2022-05-02T11:57:05	2	IDS	ET POLICY HTTP Host header contains known malicious domain	Clients	OUT	0.35	26	0.6	5	0	0	0
2022-05-02T11:57:05	3	IDS	ET POLICY HTTP Traffic to known malicious IP address	Clients	OUT	0.2	5	0.33	6	0	0	0
2022-05-02T11:57:05	4	IDS	ET POLICY DNS Query for known malicious domain	Clients	Servers	0.12	26	0.12	26	21	2.3883	10.46154
2022-05-02T11:57:06	1	SIEM	Malicious domain traffic detected	Clients	Servers	0.14	14	0.33	3	21	2.3883	10.46154
2022-05-02T11:57:06	2	SIEM	Phishing Victim detected downloading malicious file	OUT	Clients	0.08	12	0.14	14	21	2.3658	9.384615
2022-05-02T11:57:06	3	SIEM	Malicious domain traffic detected	Servers	OUT	0.07	14	0.08	12	0	0	0
2022-05-02T11:57:06	4	SIEM	Malicious domain traffic detected	Clients	OUT	0.07	14	0.08	12	0	0	0

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

www.Cyber-MAR.eu

Cyber_MAR

Cyber-MAR EU Project

Cyber-MAR

info@lists.Cyber-MAR.eu

THANK YOU FOR YOUR ATTENTION

Markos Antonopoulos, ICCS

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