SMS-I: an Intelligent Correlation tool for Cyber-physical Systems*

Eva Maia[1][0000-0002-8075-531X], Norberto Sousa[1][0000-0003-2919-4817], Nuno Oliveira[1][0000-0002-5030-7751], Sinan Wannous[1][0000-0002-9711-4850], and Isabel Praça[1][0000 0002 2519 9859]

GECAD - Research Group on Intelligent Engineering and Computing for Advanced Innovation and Development, School of Engineering of the Polytechnic of Porto (ISEP), Porto, Portugal. {egm,norbe nunal,sinai,icp}@isep.ipp.pt

Abstract. Airports, like other critical infrastructures, are an attractive target for attackers, mainly due to the catastrophic impact of these attacks on society. In addition, the cyber-physical nature of airports makes them more vulnerable to cyber-physical threats, and makes detecting and investigating security attacks more difficult. Therefore, it is important to improve cyber-physical correlations and forensics investigations at airports. This work describes the SMS-I tool that allows the improvement of these two aspects at airports. Data from heterogeneous systems, over different time frames, are received and correlated. Both physical and logical security are unified and additional security details are analysed to find attack evidence. Different Artificial Intelligence (AI) methodologies are used to process and analyse the multi-dimensional data exploring the temporal correlation between cyber and physical alerts and going beyond traditional techniques to detect unusual events, and then find evidence of attacks. SMS-I's Intelligent Dashboard supports decision makers in a deep analysis of how the breaches and the assets were explored and compromised. It assists and facilitates the security analysts using graphical dashboards and alert classification suggestions. Therefore, they can more easily identify anomalous situations that can be related to possible incident occurrences. Users can also explore information, with different levels of detail, including logical information and technical specifications.

Keywords: Cyber-physical Systems· Digital Forensics · Cyber-physical Systems Forensics· Machine Learning · Rule Mining.

1 Introduction

Airports are complex critical infrastructures composed by multiple systems that allow the transit of thousands of people every day. Their importance and criticality in today's society makes them an attractive target for attackers. Therefore,

* This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 832969. This output reflects the views only of the author(s), and the European Union cannot be held responsible for any use which may be made of the information contained therein. For more information on the project see: http://satie-h2020.eu/.

airports face daily challenges to ensure the business continuity and the passenger's safety. Despite the fact that airports are usually well protected against individual cyber threats and in some cases protected against certain physical attacks on individual systems, a remaining major issue is the vulnerability to combined cyber-physical threats. Thus, the SATIE project aims to build a security toolkit [9] in order to protect critical air transport infrastructure against combined cyber-physical threats, by improving the cyber-physical correlations, forensics investigations and dynamic impact assessment at airports.

Cyber-physical systems (CPS) combine the physical and cyber worlds, which allows an improvement of the entire operating environment by adding different promising capabilities to these environments [10]. Therefore, CPS are being used in several domains including manufacturing processes, healthcare, transportation, and commercial and residencial smart buildings [5]. This can happen because CPS use and integrate different technologies, from software systems, networks and sensors to hardware devices such as microcontrollers and actuators. However, this combination enabling interactions between cyber and physical components, not only brings new paths of attack but also increases the attack impact, since an event caused by a cyber component can have a huge impact on physical ones or vice-versa [12]. Thus, beyond damage to cyber and physical components, a cyber-physical attack can also have major consequences that may include human deaths and injuries, infrastructure damages, loss of resources, and machine breakdowns or malfunctions. These damages can have an even greater impact on critical infrastructure such as hospitals and airports. Stuxnet worm [8], the US power grid attack [17], German steel-mill incident [3], the Ukrainian power grid incident [11], and the recent Florida Water Treatment Plant [7] and Colonial Pipeline [19] attacks, are some examples of security attacks on CPS that have caused huge impacts on the normal operation of the systems.

After an attack it is crucial to understand how the attack was performed, who did the attack and why the attack happened. This will help to understand which assets were compromised but also will allow the creation of defense mechanisms for future attacks. For that security analysts need to analyse and investigate several sources of information. In CPS, this investigation process becomes much wider and complex, due to the amount of components that need to be analysed. Not only software and hardware components need to be considered but also all interactions across all CPS. Several investigations have been done to develop tools to secure CPS as well as techniques and frameworks to evaluate CPS security, however CPS forensic investigation area is still in its early stage. Mohamed et al. [14] reviewed examples of current research efforts in the field and the types of tools and methods proposed for CPS forensics. The authors also discussed some issues and challenges in the field that need to be addressed. One of the issues pointed out was the need for data analytics tools to find correlations between digital and physical evidence.

In this work we describe the SMS-I tool which deals with the analysis of data from heterogeneous systems, over different time frames and correlates them to

find evidence of the causes of an attack, allowing the improvement of the forensics investigation at airports. It analyses additional security details, providing contextual and semantic data, to identify causes for security events and threats. Machine Learning (ML) methodologies have been applied for outlier detection, exploring the temporal correlation between cyber and physical alerts, and going beyond traditional one-class algorithms, and considering ensemble methods to detect unusual events, taking into account its sequential nature, which may help to find evidence of attacks. An intelligent dashboard is also part of the SMS-I in order to support decision makers in a deep analysis of how the breaches and the assets were explored and compromised. A first overview of this tool was presented in [13].

2 SMS-I Tool Overview

SMS-I is a forensics investigation system that is a part of the SATIE security toolkit. In the SATIE security environment, cyber and physical sensors are scattered across the whole airport's infrastructure collecting vast amounts of events related to the airport system's activity. These events are sent to the CEngine, a pattern matching mechanism that contains expert written rules which are periodically reviewed and updated under a strict protocol, to possibly identify abnormal behaviour. When a set of events trigger a specific rule, an alert is originated and sent to the incident Management Portal (IMP). In the IMP, after investigating the alert occurrence, the security operator classifies alerts as either incidents or not, triggering a security response. SMS-I tool inspects these incident and alert occurrences to provide a deeper analysis of an attack. For that, the system periodically fetches data from the CEngine and the IMP using HTTP(S) requests to obtain alerts and incidents generated by the SATIE Toolkit. This data is parsed into predefined formats and stored into specific indexes of the SMS-I Database. This is a crucial part of the SMS-I tool since it allows the system to keep track with the new data that is generated within the SATIE Environment. Then, the SMS-I ML Engine gets this new data and executes the ML models capable of determining, for each alert, the probability of it being an incident based on its own features, features of related events and the features of other alerts of a regarded time window. The employed models are expected to grow smarter over time with system usage. Additionally, using the Association Rule Mining (ARM) Engine, the SMS-I ML Engine provides an API endpoint for executing rule mining algorithms on the SMS-I Database data according to a set of parameters specified in the request header. It retrieves the list of association rules to identify probable relationships between alerts for a given timeframe. Finally, the SMS-I Intelligent Dashboard provides a Graphical User Interface of all this data that handles the interaction with the security analyst. It encapsulates Kibana dashboards and allows the operator to make use of several functionalities such as consulting alert lists, performing filtering, mining new association rules, managing association rule base and consulting alert details. An overview of the SMS-I architecture can be seen in Fig. 1.

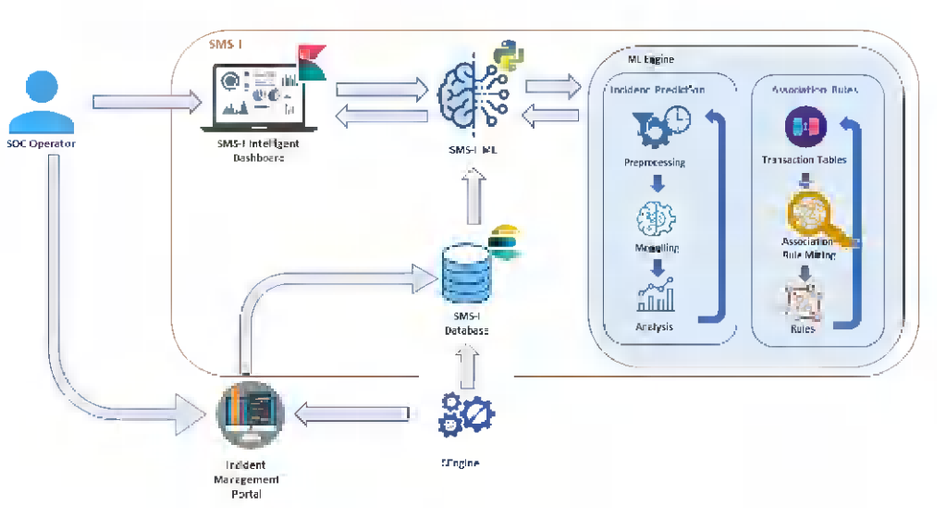

Fig. 1. SMS-I architecture overview

3 SMS-I Machine Learning Engine

The ML methods present in the SMS-I can be categorized into two groups: incident probability prediction and association rule mining. For the first, supervised algorithms were trained on the sequential data of cyber and physical alerts to predict the probability of a given alert to be an incident based on previous occurrences. On the other hand, the second group of methods uses the same data to derive new correlation rules between alerts that can be analysed to understand the complex pattern inherent to such data. Both will be described in the following sections.

3.1 Incident Probabilities

There are many approaches for building ML models that can efficiently detect anomalies in time series data. To properly investigate and explore state of the art methods for such task a study on public datasets was performed. One of the difficulties of this study was to find an appropriate testbed for testing the employed methods performance. The lack of good and reliable datasets has been appointed in the literature as one of the main obstacles in intrusion detection research [18]. However some datasets have been recently introduced to solve this issue, NSW-NB15 [15], CICIDS2017 [21] and CIDDS-001 [18]. From all the previously mentioned, CIDDS-001 was the one selected to be used for several reasons such as the number of records, the recording period duration and the considered attack types. Therefore, anomaly detection for the CIDDS-001 dataset, considering the AttackType label, was addressed using two different approaches: single-flow and multi-flow. The first regards individual flows as separate records and attempts to find differences between normal and attack related ones. The

later, considers a given window of flows performing an analysis on the entire data sequence to detect anomalies. For each approach three ML algorithms were experimented and compared: Random Forest (RF), Multi-player Perception (MLP) and Long-Short Term Memory (LSTM). The results [16] shown that considering the single-flow approach the best performing model was the RF with an F1-score of 85.04%. For the multi-flow approach, the best f1-score value, 91.66%, was obtained by the LSTM model for a window size of 70. Although the performance of the RF considerably drops with the increase in sequence length, for a window size of 10, it achieved a f1-score of 89.82%, which is relatively close to the best recorded value. From the results, it can be concluded that learning sequential relationships between flows seem to improve anomaly detection considerably. The LSTM has proven to be a very reliable model for capturing these sequential patterns, and its performance appears to get better for bigger flow sequences.

After the training using a public dataset, a SATIE dataset was used to fine tune the incident probability algorithm. The normal use of the SATIE Toolkit and the scenario simulations generated allowed the creation of the SATIE dataset. All the alerts related to incidents, 368, were labelled as malicious while the remaining ones, 9215, were marked as normal. Despite this dataset is not large in terms of data volume and has a high-class imbalance since more than 96% of records are benign, these experiments were important to understand which approaches are better for the SATIE data and how well can the algorithms distinguish between malicious alerts, which were tagged as incidents, and false positive alerts. However, these dataset characteristics made the application of deep learning approach such as MLP and LSTM unviable. Additionally, there were multiple challenges regarding data quality such as alerts related to incidents that were not manually labelled in the IMP, alerts with a lot of empty fields that were only generated to test SATIE Tools and many repeated entries due to simulations that are executed daily. To mitigate these problems, every feature with over 60% missing values were discarded as well as all the alerts related to the repeated daily executions. Furthermore, an oversampling method, Synthetic Minority Oversampling Technique was used to produce synthetic examples of incidents to minimize the class imbalance. The data, after being pre-processed, was split into two sets: 70% for training and 30% for test. Then, a RF model was used as classifier (RF-1), obtaining an accuracy of 98.08%. However, the value of F1-score, 60.94%, indicated that the model was performing poorly on the minority class, failing to classify most of the incidents. In an attempt to improve the obtained results, three time-based features were engineered for a given window of time (30 minutes), the number of alerts, the number of distinct sensors and the most common sensor. With the new features, both accuracy and F1-score of this new classifier (RF-2) improved significantly, 98.54% and 76.60% respectively. These results lead to believe that an approach which combines both individual alert features and time-based engineered features can work quite well on the SATIE data.

3.2 Association rule mining

Apriori is a very popular algorithm for data mining focusing on association rules, developed by Agrawal and Srikan in 1994 [1]. It identifies the items or patterns in a transactional dataset and then relates frequent occurrences to those patterns, generating association rules to describe them [6]. These rules are comprised of statements that describe the relationships between seemingly unrelated items inside a transaction. Let $X = \{i_1, 1_2, \ldots, i_m\}$ be the set of all items concerned in a dataset, and $T = \{t_1, t_2, \ldots, t_m\}$ be a set of transactions, where each transaction is a set of items. The association rule, noted as $X \Rightarrow Y$ indicates a certain relation between two itemsets X and Y. An association rule $X \Rightarrow Y$ is supported if the percentage of transactions that contain both itemset X and Y in T exceeds a certain threshold, called support thresholdFurthermore, the confidence for the association rule $X \Rightarrow Y$ is defined by the percentage of transactions that contain itemset Y among transactions containing itemset XThe support represents the usefulness of the discovered rule and the confidence represents certainty of the rule. Lift is a simple correlation measuring whether X and Y are independent or dependent and correlated events. If a rule has a lift of one, X and Y are independent and no rule will be generated containing either event. If a rule has a lift greater than one, X and Y are dependent and correlated positively.

To build the association rule mining for SMS-I tool, using the apriori algorithm, the sequences of alerts in a mineable database were grouped by using a certain criterion to form transactions. That criterion is a time window, and the focus will be the name of the sensor that originated the alert. In order to compile the transactional dataset, for each alert the selected window was subtracted to its "detect_date" field. From the obtained time range, all alerts that fell inside that interval were joined and a list with their sensor's name was created, performing this operation to all entries, obtaining the set of transactions. Using this set of transactions several rules are generated to be allow the user to understand the correlation of the different sensor alerts in an attack.

4 SMS-I Intelligent Dashboard

SMS-I allows the analysis of data from heterogeneous systems, over different time frames. To provide this information regarding the system's events, alerts, and incidents in a useful way, it implements a visualization tool - the SMS-I Intelligent Dashboard. It assists and facilitates the security analyst's work using graphical dashboards and alert classification suggestions, which derive from the SMS-I ML Engine previously presented. For that, two different detailed dashboards were accessible: alerts and incidents dashboards. Both were developed using Elasticsearch and Kibana technologies. Elasticsearch is responsible for the analysis, normalization, enrichment and storage of alert and incident data, as well as data provided by ML algorithms. Then, this data is the accessed by Kibana to create these two dashboards, which allows the user to search and visualize airport security related data.

The Alerts Dashboard includes all data related to airport security alerts generated by the different cyber and physical Threat Detection Systems available in the SATIE Toolkit. One of the main goals of this dashboard is to monitor the quantity, nature, and severity of alerts, considering their incident prediction probability, which is calculated by the SMS-I ML Engine. More than 70% of security analysts feel overwhelmed with the number of alerts and incidents they need to investigate for a day [2]. More than 50% of organizations receive over 10,000 alerts daily, which can lead to alert fatigue and neglect. So, to maintain SOC efficiency and reduce the impact of the investigation on the responsible personnel, it is essential to control the quantity of received alerts and incidents. Therefore, a set of graphics and metrics were added to this dashboard (see Fig. 2) to monitor the quantity of alerts received to help avoid a sudden overload of alerts by monitoring the total number of cyber and physical alerts. The severity of

Fig. 2. SMS-I Intelligent Dashboard: Alert quantity monitoring visualizations

alerts is another important parameter that needs to be monitored by security analysts, since alert's severity defines if the alert should be ignored or if there is a need to carry out a more thorough investigation. For the SATIE project, four severity levels were defined: high, medium, low, and info. Besides controlling the number of alerts for each severity level, to avoid the overburdening of security analysts, using alerts dashboard is also possible to monitor the date of occurrence of alerts.This is useful to perform pattern and trend identification and to study previous incidents and preceding alerts. The results provided by the ML engine regarding the incident prediction probability, in other words the probability of an alert representing an incident, can also be visualized in the alerts dashboard. The most common source and target IPs and ports are also displayed to the user in the Alerts Dashboard. This information can be very valuable for the security analyst, as it helps to discover information about the attacks, namely where they come from and what the targets are.

The Incidents Dashboard aggregates all detected incidents related to airport security. This dashboard follows the structure of the Alerts Dashboard by monitoring the quantity, nature, and severity of incidents. Thus, similar to what happens with the Alerts Dashboard, it has similar visualizations available to the user, displaying information regarding incident quantity monitoring and incident severity monitoring.

SMS-I intelligent dashboard also makes available a set of different visualizations. Events timeline is one of them. It provides ability to security analysts to preview a timeline of events within the system. Events are displayed in the form of an ordered timeline, with summarized info of each event (Fig. 3). Filters can be applied to customize the timeline, such as: maximum alerts number, minimum incident probability, and time range. A Watch List section is also

Fig. 3. SMS-I Intelligent Dashboard: Events timeline

available and allow users to preview a list of the latest alerts within the system. Alerts in this list are being displayed in the form of aligned cards, with summarized info of each alert within the corresponding card. The list can be sorted by detection time or incident probability, and filtered by maximum alerts number, minimum incident probability, and time range. Each card within the list has highlights of the alert details. Users can click on any card to display the full details of the corresponding alert (Fig. 4). Furthermore, cards are displayed using indexed colours that reflect the severity level of each alert (red for High, orange for Medium, and Green for low). When the user clicks on a specific alert Card, the corresponding alert details will be displayed. Details include the alert title and description, information identifying the alert, the source and target details, and the probability of this alert being an incident. If the card is a specific incident Card, the corresponding incident details as well as the related alerts will be displayed (Fig. 4).

Another important part of SMS-I Intelligent Dashboard is the Association Rules functionality (Fig. 5) which allows security analysts to automatically generate rules that can help them understand, using historical data, the correlation of the different sensor alerts in an attack. The security analyst can customize the parameters, namely the time window, the support and confidence, to generate different rules.

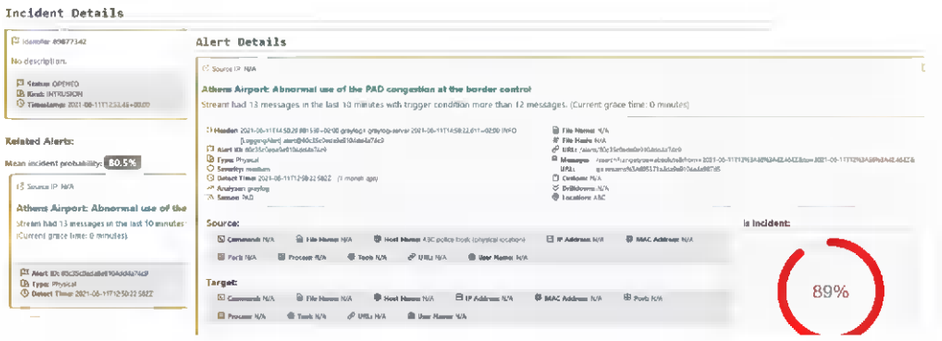

Fig. 4. SMS-I Intelligent Dashboard: Incident and Alert details example

Fig. 5. SMS-I Intelligent Dashboard: Association rules visualization

5 SMS-I Demonstration

Three different airports from three different countries are part of the SATIE project to ensure that SATIE security toolkit is scalable and adaptable to the operational needs, and compliant with the emerging regulations and standards at national and European levels. For that, the entire SATIE Solution was embedded into a validation environments. First, a simulated environment where the SATIE solution and the airport and ATC systems are fully virtualized was used. Then three demonstrations at the airport sites were made, where the SATIE solution implemented in the simulated environment was connected with the actual airport systems (as far as possible). Five different threat scenarios were defined to be performed in the validation environments. They were fine-tuned to take into account the technical performances and configurations of the actual airports' systems and operational requirements. The scenarios were also customized to be feasible on the simulation platform and in each airport environment.

During the two different validation phases, using the the simulation platform and in the pilot sites, different security analysts used SMS-I tool, through the SMS-I Intelligent Dashboard. This interaction allowed the fine tuning of the tool, gathering more data to refine the SMS-I ML engine, but it also highlighted the need to have tools, like SMS-I, that correlate the different cyber and physical security alerts. IBM stated that it took an average of 287 days to identify and contain a data breach in 2020 [20]. This detection time demonstrates how difficult is for companies to detect and mitigate cyber atacks [22]. Moreover, the analytic tasks conducted by security analysts rely heavily on a cognitive decision-making process that can differ between analysts, depending on their technical knowledge or level of experience [4]. This is why it is so important to have intelligent tools to support security analyst decisions. In one of five different threat scenarios used to perform validation of the SATIE Toolkit, an attacker seeks to perform cyber attacks on the Airport Operation Control Center (AOCC) system to manipulate the information displayed in the Flight Information Display System (FIDS) to trigger odd passenger movements to cause an ideal hostage situation, and odd plane movements on the platform to create a fatal collision. For that the attacker sends a spear-phising email to a computer with administrator privileges in the AOCC room. An AOCC employee opens the email on that computer and clicks on the link which allows the malware to be downloaded and executed. This malware allows the attacker to take remote control of the computer. Then, the attacker performs a network scan to determine the network address and port of the Airport Operation Database server – his main target. From a security analyst's perspective, it is important to correlate both events and understand that they are steps of the same attack. However, during the demonstration of this scenario the security operator reported the corresponding alerts as two different incidents (Fig. 6). Moreover, the port scanning alert was classified as a low severity incident, which should not be the case since it is already the second stage of the attack. Using the SMS-I Intelligent Dashboard, after the reporting of the incident by the security operator, the security analyst can observe that, despite this was an incident that was reported as a low severity incident, it is related with an alert that has a 69% probability of being an incident (Fig. 6), thus it should be reported with higher severity. Furthermore, using association rules, the security analyst can understand that malware alert and the network scan alert are correlated and should be reported as being part of the same incident. This is just a "real" and very simple example that illustrates the need of intelligent tools that can help security analysts in their decision-making process.

6 Conclusion

This work describes the SMS-I tool that allows the improvement of the forensics investigation at airports. It is a complex system composed by multiple components with specific functions, namely periodic data synchronization, incident probability, association rule mining, dashboard visualization and a several other functionalities involving different lists and filters. Several AI approaches were

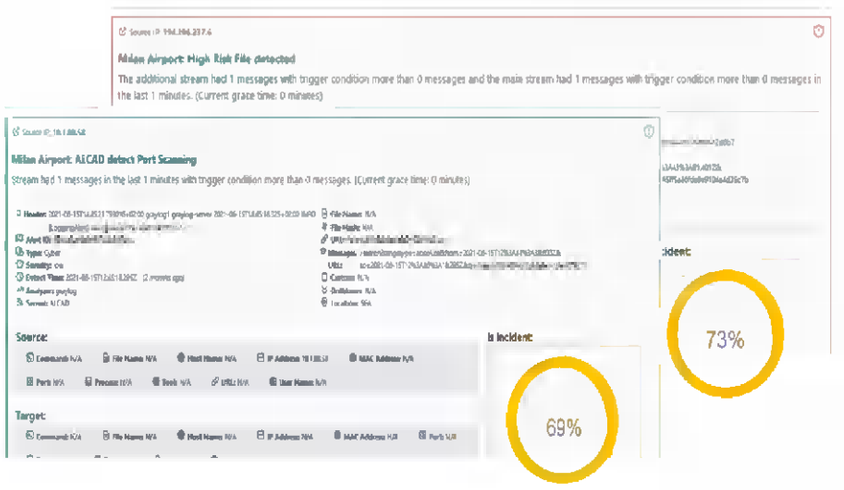

Fig. 6. SMS-I Intelligent Dashboard: Malware Detection by Malware Analyser and Network Scan detection by ALCAD system (part of SATIE toolkit)

used to process and analyse the multi-dimensional SATIE platform data exploring the temporal correlation between cyber and physical alerts. Supervised algorithms were trained on the sequential data of cyber and physical alerts to predict the probability of a given alert to be an incident based on previous occurrences. The results obtained suggest that the multi-flow approach outperforms the single-flow-based one and that the LSTM is a robust algorithm to understand complex patterns in sequential data, in particularly, network traffic data. Also, several association rules can be created applying different ML techniques, that allows the user to understand the correlation of the different data in an attack.

All the information can be visualized in the SMS-I Intelligent Dashboard. Several graphical dashboards, with different level of detail, can be used to easily identify anomalous situations that can be related to possible incident occurrences. Also, the information provided by the ML algorithms, namely the incident probability can be analysed on SMS-I intelligent dashboard. Moreover, for an additional insight about the association rules, a management of the association rules by the security analysts can also be done.

SMS-I tool was tested in three different European airports: Milano Malpensa Airport, Athens International Airport and Zagreb Airport. The tests allowed the improvement of the AI modules and the fine-tuning of the different visualizations. In this work, a very simple and authentic example demonstrated the convenience and usefulness of the SMS-I tool in the decision-making process of security analysts. As future work, we plan to test SMS-I in other airports as well as try to adapt it to other cyber-physical systems.

References

1. Agrawal, R., Srikant, R.: Fast algorithms for mining association rules in large databases. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA (1994)
2. Casey, T.: Survey: 27 percent of it professionals receive more than 1 million security alerts daily (May 2018), https://www.imperva.com/blog/27-percent-of-it-professionals-receive-more-than-1-million-security-alerts-daily/
3. Colatin, S.D.T.: Steel mill in germany (May 2014), https://cyberlaw.ccdcoe.org/wiki/Steel_mill_in_Germany_(2014)
4. Daniel, C., Gill, T., Hevner, A., Mullarkey, M.: A deep neural network approach to tracing paths in cybersecurity investigations. In: ICDMW. pp. 472–479 (2020)
5. Gunes, V., Peter, S., Givargis, T., Vahid, F.: A survey on concepts, applications, and challenges in cyber-physical systems. KSII TIIS **8**, 4242–4268 (2014)
6. Han, J., Kamber, M., Pei, J.: Data mining concepts and techniques, third edition
7. Kardon, S.: Florida water treatment plant hit with cyber attack (Feb 2021), https://www.industrialdefender.com/florida-water-treatment-plant-cyber-attack/
8. Karnouskos, S.: Stuxnet worm impact on industrial cyber-physical system security. IECON 2011 pp. 4490–4494 (2011)
9. Köpke, C., *et al.*.: Impact propagation in airport systems. In: CPS4CIP. pp. 191–206. Springer International Publishing, Cham (2021)
10. Lee, E.A.: Cyber physical systems: Design challenges. In: 2008 11th IEEE ISORC. pp. 363–369 (2008). https://doi.org/10.1109/ISORC.2008.25
11. Lee, R.M., Assante, M.J., Conway, T.: Analysis of the cyber attack on the ukrainian power grid. E-ISAC (2016)
12. Loukas, G.: Cyber-physical attacks: A growing invisible threat (2015)
13. Macedo, L., Wanous, S., Oliveira, N., Sousa, O., Praça, I.: A tool to support the investigation and visualization of cyber and/or physical incidents. In: Rocha, Á., *et al.*. (ed.) WorldCIST. Springer International Publishing (2021)
14. Mohamed, N., Al-Jaroodi, J., Jawhar, I.: Cyber–physical systems forensics: Today and tomorrow. Journal of Sensor and Actuator Networks **9**(3) (2020)
15. Moustafa, N., Slay, J.: Unsw-nb15: a comprehensive data set for network intrusion detection systems (unsw-nb15 network data set). In: 2015 MilCIS. pp. 1–6 (2015). https://doi.org/10.1109/MilCIS.2015.7348942
16. Oliveira, N., Praça, I., Maia, E., Sousa, O.: Intelligent cyber attack detection and classification for network-based intrusion detection systems. Applied Sciences **11**(4) (2021)
17. Plumer, C.: It's way too easy to cause a massive blackout in the us (Apr 2014), https://www.vox.com/2014/4/14/5604992/us-power-grid-vulnerability
18. Ring, M., Wunderlich, S., Grüdl, D., Landes, D., Hotho, A.: Flow-based benchmark data sets for intrusion detection (2017)
19. Sanger, D.E., Krauss, C., Perlroth, N.: Cyberattack forces a shutdown of a top u.s. pipeline (May 2021), https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html
20. Security, I.: Cost of a data breach report 2021 (July 2021)
21. Sharafaldin., I., Habibi Lashkari., A., Ghorbani., A.A.: Toward generating a new intrusion detection dataset and intrusion traffic characterization. In: Proceedings of the 4th ICISSP,. pp. 108–116. INSTICC, SciTePress (2018)
22. Vielberth, M., Böhm, F., Fichtinger, I., Pernul, G.: Security operations center: A systematic study and open challenges. IEEE Access **8**, 227756–227779 (2020)