Towards a Human-in-the-Loop Intelligent Intrusion Detection System

Evita Roponena[*,†,1], Jānis Kampars[†,1], Jānis Grabis[†,1] and Andris Gailītis[†,2]

[1] *Riga Technical University, Zunda Krastmala 10, Riga, LV-1048, Latvia*
[2] *SIA "Izglītības sistēmas", Cuibes iela 17, Riga, Latvia*

Abstract

Information and communication technologies are an essential part of almost any business sector and, therefore, are the target of different cyberattacks. ICT security measures are necessary to protect information from unauthorized access. The Human-in-the-Loop approach argues that cybersecurity specialists should be continuously involved in evaluation of automated intrusion detection activities and should be supported by suitable tools to evaluate the situation. This paper proposes an overall design of the intelligent intrusion detection system with a focus on supporting cybersecurity specialists to fulfill the requirements of the Human-in-the-Loop approach. Typical users of cybersecurity, their use cases and interactions are identified. Architectural components supporting implementation of the system are identified. Big data and machine learning threat identification, knowledge management and personalized workplaces for system administrators and other users are the key modules of the system.

Keywords

Intrusion Detection, cybersecurity, big data, human factors

1. Introduction

Information and communication technologies (ICT) are an essential part of any business sector. These technologies are used to automate business processes, to store and process data, which can also include sensitive information. Therefore, data access by unauthorized third parties or cyberattacks on the system can cause a disruption of business processes or even cause permanent damage to the system itself. With the growing dependence on ICT technologies, there is a growing potential for significant damage to public administration IS and electronic communications networks, neutralization of national politics, economics, and military decision-making centres, misinformation of the public and the emergence of man-made technogenic accidents, leading to a growing risk of non-military threats with severe consequences.

Data centres are typically used as a host for various ICT systems, and therefore are typical targets of cybercriminals and security threats. According to [1], threats such as viruses, malware, ransomware, spyware, spam, phishing, DDoS, and other related threats are frequent in data centres, which shows the importance of real-time network monitoring and threat prevention. According to the report [2], phishing threats increased from 3% in 2018 to 9% in 2019, and also the amount of compromised data has increased. In 2019 botnet C2 servers number has increased by 57% compared to 2018, which are usually associated with distributed denial of service (DDoS) attacks [3]. Timely intrusion detection and response is essential to dealing with these threats.

However, continuous monitoring of enterprise IS and network data, as well as incident identification and threat prevention, impose serious performance and scalability requirements on the ICT security

Baltic DB&IS 2022 Doctoral Consortium and Forum, July 03-06, 2022, Riga, LATVIA

* Corresponding author.

† These authors contributed equally.

EMAIL: evita.roponena@rtu.lv (E. Roponena); janis.kampars@rtu.lv (J. Kampars); grabis@rtu.lv (J. Grabis), info@e-klase.lv (A. Gailītis)
ORCID: 0000-0002-0309-4730 (E. Roponena); 0000-0003-0045-5593 (J. Kampars); 0000-0003-2196-0214 (J. Grabis)

management solution. Currently, the most commonly used security management solutions address this issue by processing only a portion of the available data, because it would not be possible to provide the desired performance and response time when processing all data. ICT security management solutions available on the market have limited capabilities to provide a full-scale complex analysis of IS systems, network data, server logs, and other unstructured and semi-structured data; therefore, it is only possible to provide a limited level of security threat identification and appropriate action to mitigate the impact of cybersecurity incident.

Lack of cybersecurity specialists is another problem [4]. Currently, the management of ICT security incidents is performed by security personnel, and the identification of the causes of the incident and the speed of response depends directly on the experience and competence of the professionals. They need in-depth knowledge of networks, their protocols and devices, device architecture, vulnerabilities, as well as cybersecurity tools and the effectiveness of their application. Big data technologies and machine learning approaches are promising to automate intrusions detection. However, involvement of human decision-maker is still important [5]. The Human-in-the-Loop Security Model argues that automated machine learning based approaches should be combined with manual intervention models to deal with low confidence problems. Therefore, a user-oriented intrusion detection system that combines automated detection techniques with user-friendly approaches to visualize, explain, and share intrusion detection data is needed.

The objective of this paper is to propose an overall design of the intelligent intrusion detection system with the focus of supporting cybersecurity specialists to fulfil the requirements of the Human-in-the-Loop approach. Typical users of cybersecurity, their use cases and interactions are identified. Architectural components supporting implementation of the system are identified. The work is conducted as a part of university and industry collaboration applied research project, and the results will serve as basis for further implementation of the system. The proposed system is known as BICTSeMS.

The rest of the paper is organized into 5 sections. Characteristics of current intrusion detection systems are reviewed in Section 2. The requirements are identified in Section 3. The overall design of the proposed systems is presented in Section 4. Section 5 contains the conclusion, and section 6 - acknowledgments.

2. Background

Intrusion detection systems (IDS) monitor network traffic by scanning a network or a system to identify suspicious activity and generate alerts when suspicious activity is discovered. Measurement criteria as the false positives (unmalicious activity identified as malicious), false negatives (malicious activity identified as unmalicious) are used to evaluate IDS performance.

IDS can be classified into five types:

1. Network-based IDS (NIDS) - monitors packets from the network,
2. Host-based IDS (HIDS) - analyse the audit data of the operation system,
3. Protocol-based IDS (PIDS) - is located in the front end of a server and controls and interprets the protocol between user/device and server to secure a web server,
4. Application protocol-based IDS (APIDS) - is located in a group of servers and monitors and interprets the communication on application specific protocols,
5. Hybrid IDS which is a combination of two or more approaches.

IDS uses two different detection methods: the signature-based method or the misuse detection and the anomaly-based method. Misuse detection identify attacks based on specific patterns or signatures. It uses information on previously detected malware. One of the signature-based IDS main problems is large number of signatures in the database, which leads to possible misses of dangerous attacks and inability to detect unknown attacks. The anomaly-based method uses machine learning to detect previously unknown malware. The disadvantage of this method is that non-malicious behavior can be identified as an incident that leads to high false positives rate. Both intrusion detection methods can be combined to overcome the disadvantages of these methods [6]. In various research papers, IDS are supplemented with additional methods to improve IDS performance and overcome its limitations.

The new generation IDS that can correlate information from various resources to identify bots in the network before they inflict damage is proposed by [7]. The solution consists of the Snort network intrusion detection system that performs real-time traffic analysis and packet logging and Splunk that identifies data captures, correlates real-time data, and generates visualizations.

The Signature Apriori algorithm can be used to implement the misuse detection technique and data mining into IDS. The main concept of the algorithm is to use prior knowledge of the properties of the frequent itemset. This method is used in [8] research with an additional Scan-Reduction method to minimize scans of the database and by the observation of the attack signatures determine which attack signatures depend on each other and identify the new attacking signature. The system analyses data gathered from Snort and packet sniffer to find frequent items which meet minimum support, and afterwards checks all possible combinations with already known signatures. The proposed algorithm is faster than the Signature Apriori algorithm with a moderate false positive rate ~25%.

Open-Source Intelligence (OSINT) is a technique that may be used to automatically update IDS knowledge by collecting knowledge about threats from diverse sources. In [9] the OSINT data are used to generate rules and blacklists that are later integrated into an IDS in the IDSoSint prototype. The proposed approach acts continuously in a loop, each iteration containing three phases: information gathering and categorizing into predefined threat categories, knowledge generation by correlating gathered information, and incident detection managed by Pulledpork[2] platform and updating of the Snort IDS. The proposed approach is able to successfully generate rules and blacklist entries using OSINT feeds and is able to eliminate traffic based on blacklists and then emit the remaining incidents through Snort’s rule processor.

The enhanced signature-based IDS is proposed in the research [10]. The proposed solution resolves signature-based IDS disadvantages by distributing signature database in the several small databases based on a protocol type; by using a filtering engine and by updating engine. The IDS captures an incoming packet, extracts its signature, and matches the extracted signatures with the signatures stored in the databases. If there is a match, the alert is sent and the packet is blocked; if not, the packet goes through the filtering engine which checks the similarity of the signatures of the new packet and the stored in databases, and whether the new IP is stored on the IP blacklist. If the packet passes those criteria, it is clean; if not it is blocked, and the signature databases and blacklist are dynamically updated.

[11] propose an associated graph set (AGS) model-based NIDS architecture for enterprise network. Model requires the decomposition of the host into sets of MAC addresses, IP addresses and Ports associated with the host. An address of each level can be associated with one or more addresses of neighboring levels. These sets specify a mapping function for network associations, up to the OSI protocol stack, and the analysis of these mappings allows one to define node’s internal configuration and enter security validation rules. Any attack on each OSI layer makes changes in the graph structure and can be detected. Hosts are classified according to the communication role, and the information can be used to collect data about the system. The information can be divided into structural data and communication data. The AGS NIDS architecture includes two layers of analysis modules: module to identify attacks by known data mining methods based on behavior, specifications or knowledge, module to generate the system, system behavior, and structure rules based on the first analysis.

The brief overview shows that different approaches can be used for IDS improvement, for example, by combining multiple open-source IDS systems. Table 1 shows the overview of the most popular open-source, free, and real-time NIDS or HISD that performs data analysis, and uses both anomaly-based and signature-based detection methods.

Table 1 shows that different IDS systems can be used in combination to analyze different network logs and obtain a complete picture of the incident. Each IDS system also has a different set of features that can be used; therefore, it is important to understand the requirements of the system to select the most suitable open-source solution if needed.

[2] https://github.com/shirkdog/pulledpork

Table 1
The overview of selected open-source IDS

IDS	Type	Logs	Features
Zeek IDS[3] (Bro IDS)	NIDS	SNMP traffic, FTP, DNS, HTTP activity, events	Event Engine, Policy scripts
Snort[4]	NIDS	Network traffic packets	Packet logger, sniffer, and IDS modes, Rule-based configuration, Plugin framework
OSSEC[5]	HIDS	Alterations, mail, FTP, web server data	Creation of important files checklist and validating it
Suricata[6]	NIDS	DNS, SMB, FTP, HTTP, UDP, TLS, TCP and ICMP protocols	Integration with third-party tools like Anaval, Squil, Uses rule sets
Security Onion[7]	NIDS, HIDS	Network and host logs	Focus on log management, enterprise security monitoring. Includes tools as Elasticsearch, Locstash, Suricata, Zeek and other.

The overview of current IDS improvement solutions does not show how to integrate human interactions with the cybersecurity analysis system for the creation of the Human-in-the-loop cybersecurity system. The current IDS systems focus on technical aspects while importance of usability issues has increased recently. [5] define that a Human-in-the-loop cybersecurity system should have a machine detection module, knowledge base, confidence level module, and manual intervention module. [12] states that IDS should deliver reliable predictions about potential threats, delivers easy to understand explanations about its decisions, adapt towards new challenges and does not have a negative impact on performance. They add an explainer to the classification algorithm to meet these requirements. Visualization also plays an important role in supporting the analysis and comprehension of cyber-incidents [13]. [14] specifically focus on user interactions with IDS and provide automation of configuration activities including configuration by means of using voice activated commands.

3. Requirements analysis

The requirements towards the Human-in-the-loop cybersecurity system are formulated to understand the required functionality of the proposed system. These requirements are elicited on the basis of analysis of existing intrusion detection systems (Section 2), literature review of automated cybersecurity solutions [15], IT security standards, and interviews conducted with representatives from an ICT company managing data centers.

3.1. Overall approach

The BICTSeMS platform is envisioned as an intelligent intrusion detection system supporting cybersecurity specialists. The threat prevention activity refers to the detection and blocking of malicious attacks on the ICT infrastructure (Figure 1). It is supported by best practices providing information of type of attacks and suitable response mechanisms. In order to support the cybersecurity specialists, the threat information is contextualized and represented in relation to the overall network topology uncovered and maintained using automated methods. The topology modeling describes relationships among the network's elements and explained potential attacked vectors. The component topology graphs are retrieved from a cloud computing platform using a specialised adapter. The topology

[3] https://zeek.org/
[4] https://www.snort.org/
[5] https://www.ossec.net/
[6] https://suricata.io/
[7] https://securityonionsolutions.com/

preprocessor extracts subgraphs (subsets of connected devices, such as one VLAN) from the entire topology graph and checks whether changes have occurred in the subgraphs. If changes are detected, a new version of the subgraph is saved in the Topology dataset.

The threat identification using big data analysis and machine learning methods continuously run in the background to identify new threats and generate warnings and recommendations to human decision makers. Positive warning and recommendations are documented as best practices to provide input for the treat detection. Thus, the BICTSeMS platform provides automated threats analysis, contextualization and accumulation of knowledge further used to help the cybersecurity specialists to monitor and to manage ICT infrastructure.

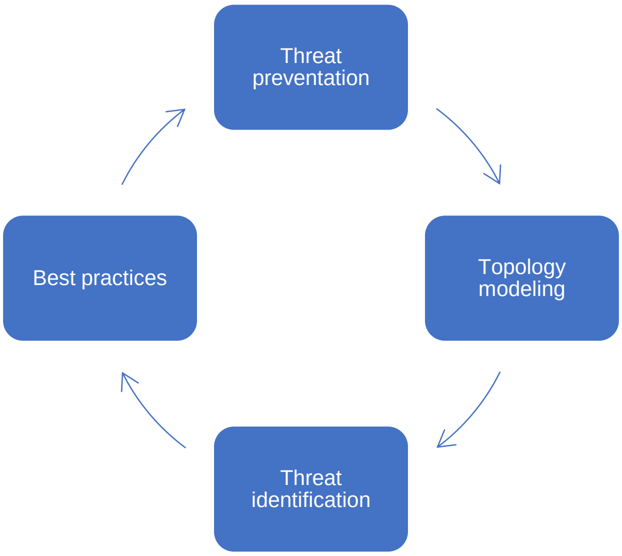

Figure 1: BICTSeMS overall approach

3.2. Uses cases

The BICTSeMS system is designed as a semi-automated system that requires human interactions to perform the security management of ICT components. The identified possible system users are the following:

1. incident response team that performs intrusion detection, advisory distribution, education and awareness, information sharing and incident response [16], it usually includes:
    a. team leader – coordinates the incident response team,
    b. lead investigator – performs evidence analysis,
    c. communication lead – provides necessary communication inside and outside of the company,
    d. documentation and timeline lead – documents team activities and tasks,
    e. legal representative – assures that incident response activities are in line with laws and regulations,
2. system administrator – responsible for the maintaining of computer systems, for example, servers,
3. BICTSeMS administrator – responsible for the BICTSeMS system user management, system performance, and system configuration.

In this system context, incident response team manages incident identification and prevention processes and maintains ICT security management best practices repository. The system administrator is responsible for the isolation of the infected system area and is responsible for enforcing the security measures of the ICT components. The system itself performs automatic data analysis, threat detection and prevention if the instant actions are needed.

The BICTSeMS system provides different functionality to maintain a high ICT security level, this functionality is summarized into five use cases:

Use Case 1: Real time full-scale integration of system data: Provides ICT system components data reception, pre-processing and aggregation used for security threat identification.

Use Case 2: Identification of security threats: Performs system cyber security threat identification based on system data analysis provided by Use Case 1.

Use Case 3: Security threat prevention: Performs cyber security threat prevention based on threat identification data.

Use Case 4: Management of ICT security management best practices repository: Provides summary of automated or recommended actions to ensure that the level of security is restored.

Use Case 5: Creation of ICT components topology model: Provides system ICT component topology model including a database with IP addresses and servers to determine the area of influence of ICT device interdependence and security incident.

Two of the use cases are described in more details in the following sub-sections.

3.2.1. Real time full-scale integration of system data

The objective of real time full-scale integration of system data is to pre-process ICT system data from various data sources (Figure 2:). The results of the analysis are passed to the BICTSeMS threat identification module for threat detection.

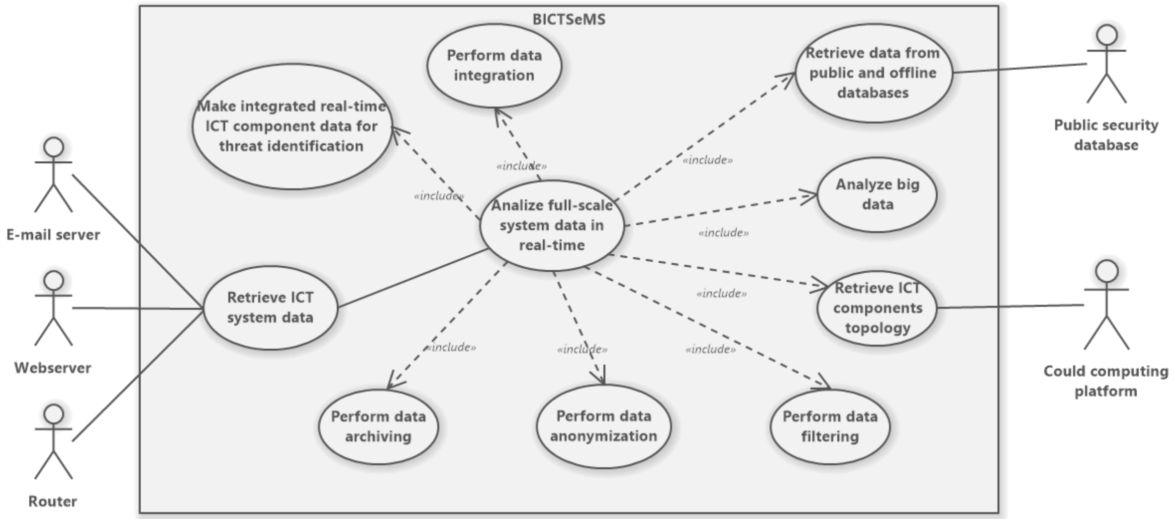

Figure 2: Use case diagram for real time full-scale integration of system data

This use case describes ICT system data analysis performed by BICTSeMS real-time data integration module using data from different sources, for example, network data, server log files, firewall log files, email log files, graph-based features, etc. that will be used to identify possible cyber security threats in the system. Data center is built on the TCP/IP network model that can be divided into four layers: physical, link, network, and application layers, and each of them has their own security risks and each of them produce different data [17]. Graph-based features represent the system components interactions, these features can be used to identify the neighbors of the infected device [18]. According to [19] usage of various data sources is important to understand the full picture of the events in the system, their correlation and sources. Therefore, the cyber security management system should be able to perform parallel processing of a huge amount of log data that have a different structure [20]. The data analysis should be done in real-time to be able to detect threats instantly and react to them [21].

Data filtering is performed to support the context of the data that is used to interpret the data and retain interesting events from large data sets. For example, by filtering data by a timeframe, the system is able to identify the correlation of the events in this timeframe, determine the attack path and it source, and exclude unrelated data. Filtering is often used in combination with prioritization that helps determine the importance of the event and whether it should be investigated [22].

The use case actors include relevant subsystems:

1. Public security database – contains IP and DNS addresses blacklists that is used for the analysis,
2. E-mail server, webserver, router – an example of data sources for full-scale system analysis,
3. Cloud computing platform – contains systems ICT components topology.

3.2.2. Creation of system components topology model

The objective of this use case is to ensure the definition of the topology model of the ICT components in the form of a graph for the further use of different components of the system (Figure 3). The use case post-conditions include making versioned ICT topology data available for other use cases.

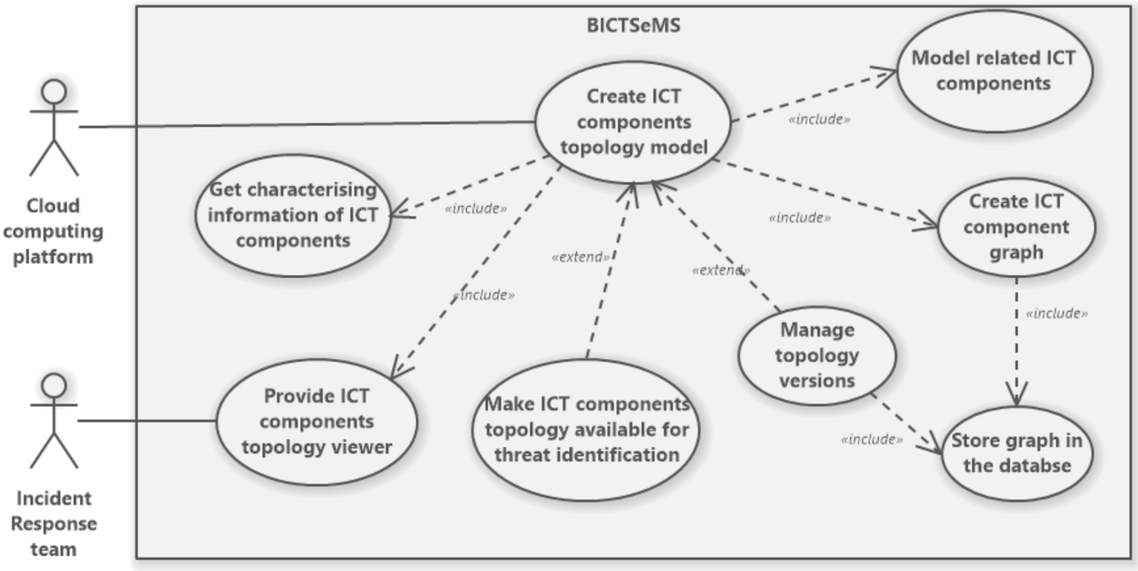
BICTSeMS
Cloud computing platform
Incident Response team
Create ICT components topology model
Model related ICT components
Get characterising information of ICT components
Create ICT component graph
Provide ICT components topology viewer
Make ICT components topology available for threat identification
Manage topology versions
Store graph in the databse
«include»
«include»
«include»
«include»
«include»
«include»
«extend»
«extend»

Figure 3: Use case diagram for the creation of system components topology model

This use case describes creation and managing of ICT components topology model. Network topology consists of nodes (users, devices, etc.), edges (relations) and degree of the node (for example, number of neighbors). The attack on certain node can cause not only disruption of this node but also could infect neighbors, therefore, topology graph is excellent way to see the relations of the nodes. When the network is large, it consists of many nodes, and it is difficult to model the interactions among all nodes. One of the solutions is to create a population game that is often used to model the strategic interaction between many players [23].

Modeling of network topology is especially helpful for botnet detection allowing to see how the network components change their connections and overall behavior [24]. Using graph-based features retrieved from network topology graph overcome the limitations of using only most common flow-based features like source and destination IPs, protocol and other that cannot capture the systems components interactions and analyze complex communication patterns [25]. For better analysis graph-based and flow-based features should be used together.

The creation of ICT component graphs contains the model of data center virtual environments (virtual machines, containers, hypervisors, etc.). The virtual environment is evolving dynamically, therefore, it is not recommended to use static topology graph for the system data analysis, threat identification and prevention, and ICT security management best practice repository. The graph is created and versioned by the graph database management system.

The use case actors include both users of the system and relevant subsystems:

1. Incident response team – views the topology of ICT components,
2. Cloud computing platform –used to create ICT component topology model.

4. Overall design

The overall design of BICTSeMS is elaborated according to the requirements following the service-oriented approach. The main components are BICTSeMS core services, infrastructure services and user interface (Figure 4). The data sources component is responsible for the capture and preprocessing of network traffic. The core services support the BICTSeMS approach and implement the specified use cases. The user interface component presents the core services to the users.

A workplace concept is used to provide a customized work environment for specific users depending on their needs. The workplace is composed of reusable components. Out-of-the-box workplaces for security manager and audit manager. The administration panel provides an overview of the current cybersecurity situation. The user interface will be developed state-of-the-art web development technologies to provide user experience customary in user-oriented applications.

The real-time data integration module provides the reception, pre-processing, and aggregation of large amounts of real-time data, obtaining the availability of information for use in machine learning models. The component interacts with the threat identification module (ensures the availability of aggregated data characterising the real-time ICT components for the performance of machine learning models). The threat prevention module, which performs automated adaptations to the ICT components or informs the responsible person in response to the identified threats and ensures the restoration of the security level, considering the topology and interdependencies of the ICT components

The ICT security management best practice repository contains automated actions or recommended actions for the responsible person to ensure that the level of security is restored in response to identified threats. The component interacts with:

1. threat prevention module - provides the selection of the most appropriate actions for the identified threats,
2. topology modelling module - defines good ICT management practices at the level of several related ICT components.

The threat identification module, which provides both specialised automated actions to identify previously known security threats (e.g., there is unauthorised port is open on the server) and machine learning models to identify previously unknown threats and identify suspicious activities in the aggregated data available to the platform. The machine learning models provides ICT components behavior patterns baselines that are created using unsupervised machine learning approach – clustering, and LSTM models. Identification of the behavior pattern of ICT components in a cybersecurity context can be used to identify abnormal activity of the by comparing the device normal activity of the device with the current activity

The topology modelling module, which ensures the definition of the topology model of ICT components in the form of a graph and the further use of the obtained graph for more accurate identification of security threats and selection of the most appropriate adaptive actions. The component that interacts with:

1. threat identification module - allows for an overview of the characterising information of ICT components,
2. threat prevention module - for performing adaptive actions in several related ICT components,
3. ICT security management best practice repository - allows to model related ICT components to formalise security management best practices.

The infrastructure services provide data streaming, messaging, data storage, and security services needed by the core services. The infrastructure services are designed using open source tools to achieve a high degree of scalability and portability. The message brokers are used for netflow data and system log streaming and service communication between each other. There are unlimited flows of netflow data and system logs. The stream processing service provides continuous data processing. The data flow is intensive, and a distributed data storage is required in order to ensure continuous data storage and analysis. Graph databases will store the network topology. The reverse proxy and load balancer on the BICTSeMS platform is expected to redirect requests to the user interface backend service, topology modelling service, the threat identification service, the threat prevention service, and the best practice repository service.

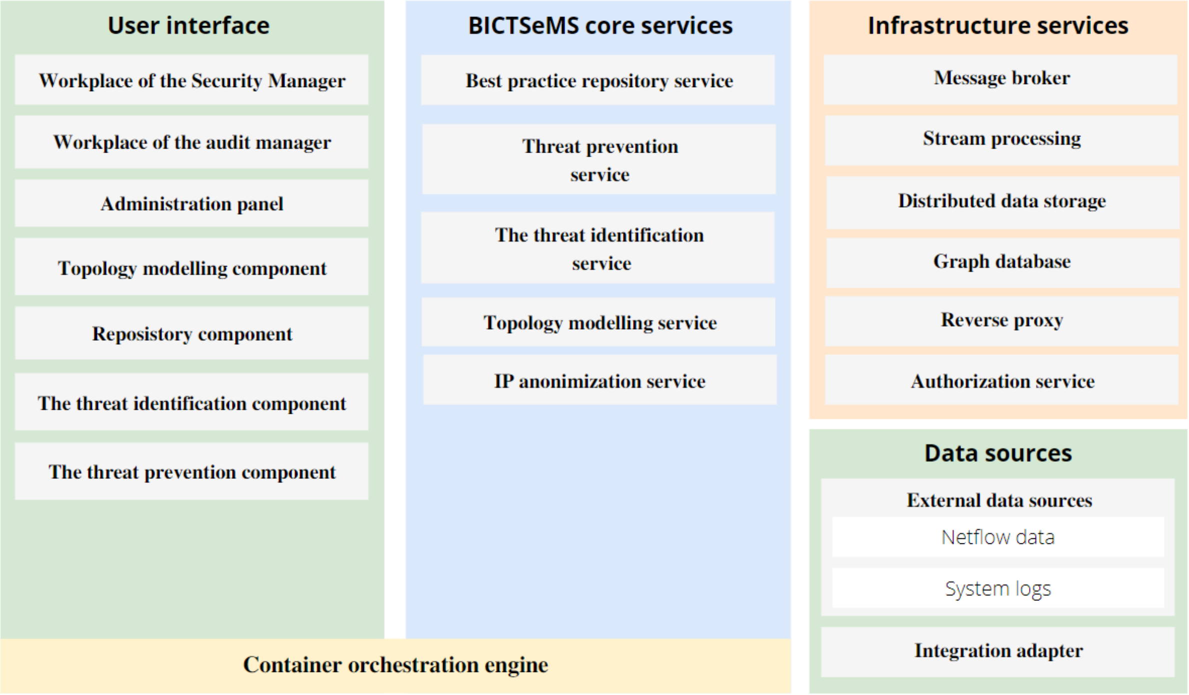
User interface
Workplace of the Security Manager
Workplace of the audit manager
Administration panel
Topology modelling component
Repository component
The threat identification component
The threat prevention component
BICTSeMS core services
Best practice repository service
Threat prevention service
The threat identification service
Topology modelling service
IP anonimization service
Infrastructure services
Message broker
Stream processing
Distributed data storage
Graph database
Reverse proxy
Authorization service
Data sources
External data sources
Netflow data
System logs
Integration adapter
Container orchestration engine

Figure 4: Overall architecture

The architecture meets the identified requirements and conforms the principles of the Human-in-the-loop security system [5]. The threat prevention and identification services implement the automated machine detection functionality. The best practice repository service provides the knowledge base. The topology modeling service provides explanatory capabilities. The users use customized workplaces in provide oversight and manual intervention module.

Technology evaluation was performed to select the most suitable technologies for BICTSeMS system development. Evaluation of criteria and 4 technology groups (network data ingest technologies, document database, real-time streaming platforms, development and analytics tools) were performed by 8 experts from Riga Technical University who are experts in software development and integration, or cybersecurity. As a result of technology evaluation, the most suitable technology for each group was obtained:

1. network data ingest technologies - software tools like GoFlow, Fprobe, and SoftFlowBD,
2. document database - Apache Cassandra,
3. real-time streaming platforms - Apache Spark,
4. development and analytics tools – Python programming language.

5. Conclusion

The paper proposes the BICTSeMS security management platform as a user-oriented solution for automated and intelligent intrusion detection. At the same time, it follows the Human-in-the-loop approach to involve human decision-makers and to support their activities. One of the key challenges is finding the right balance between automated intrusion detection and human involvement to maintain efficiency and continually develop the cybersecurity competences of users.

The BICTSeMS platform provides user friendly means to present contextualized cybersecurity information and support users with intrusion detection knowledge maintained in a best practice repository. The requirements identified and the overall architecture designed serve as the main inputs to ongoing implementation of the platform.

6. Acknowledgements

This research is funded by European Regional Development Fund Project Nr. 1.1.1.1/20/A/020 “Development of Big-data-driven Information and Communication Technology Security Management Solution (BICTSeMS)” Specific Objective 1.1.1 “Improve research and innovation capacity and the ability of Latvian research institutions to attract external funding, by investing in human capital and infrastructure” 1.1.1.1. measure “Support for applied research” (round No.4).

7. References

[1] I. Shammugam, G. N. Samy, P. Magalingam, N. Maarop, S. Perumal, and B. Shanmugam, ‘Information security threats encountered by Malaysian public sector data centers’, *Indones. J. Electr. Eng. Comput. Sci.*, vol. 21, no. 3, pp. 1820–1829, 2021.

[2] Trustwave, ‘2020 Trustwave Global Security Report’, 2020.

[3] ENISA, ‘Threat Landscape 2020 - Botnet’, 2020.

[4] ISACA, ‘State of Cybersecurity 2022: Global Update on Workforce Efforts, Resources and Cyberoperations’, 2022.

[5] Z. Zhang *et al.*, ‘Artificial intelligence in cyber security: research advances, challenges, and opportunities’, *Artif. Intell. Rev.*, vol. 55, no. 2, pp. 1029–1053, 2022.

[6] M. A. Aydın, A. H. Zaim, and K. G. Ceylan, ‘A hybrid intrusion detection system design for computer network security’, *Comput. Electr. Eng.*, vol. 35, no. 3, pp. 517–526, 2009.

[7] M. Catalin and A. Cristian, ‘An efficient method in pre-processing phase of mining suspicious web crawlers’, in *2017 21st International Conference on System Theory, Control and Computing, ICSTCC 2017*, 2017, pp. 272–277.

[8] H. Zhengbing, L. Zhitang, and W. Junqi, ‘A novel Network Intrusion Detection System (NIDS) based on signatures search of data mining’, in *Proceedings - 1st International Workshop on Knowledge Discovery and Data Mining, WKDD*, 2008, pp. 10–16.

[9] I. Vacas, I. Medeiros, and N. Neves, ‘Detecting Network Threats using OSINT Knowledge-Based IDS’, in *Proceedings - 2018 14th European Dependable Computing Conference, EDCC 2018*, 2018, pp. 128–135.

[10] M. Y. Alyousef and N. T. Abdelmajeed, ‘Dynamically detecting security threats and updating a signature-based intrusion detection system’s database’, *Procedia Comput. Sci.*, vol. 159, pp. 1507–1516, 2019.

[11] M. A. Poltavtseva, D. P. Zeghda, and E. Y. Pavlenko, ‘High - performance NIDS Architecture for Enterprise Networking’, *2019 IEEE Int. Black Sea Conf. Commun. Netw. (BlackSeaCom*, pp. 2019–2021, 2019.

[12] M. Szczepański, M. Choraś, M. Pawlicki, and R. Kozik, ‘Achieving Explainability of Intrusion Detection System by Hybrid Oracle-Explainer Approach’, in *2020 International Joint Conference on Neural Networks (IJCNN)*, 2020, pp. 1–8.

[13] A. Karami, ‘An anomaly-based intrusion detection system in presence of benign outliers with visualization capabilities’, *Expert Syst. Appl.*, vol. 108, pp. 36–60, 2018.

[14] B. Breve, S. Cirillo, and V. Deufemia, *An Intrusion Detection Framework for Non-expert Users (S)*. 2020.

[15] E. Roponena, J. Kampars, A. Gailitis, and J. Strods, ‘A Literature Review of Machine Learning Techniques for Cybersecurity in Data Centers’, *ITMS 2021 - 2021 62nd Int. Sci. Conf. Inf. Technol. Manag. Sci. Riga Tech. Univ. Proc.*, 2021.

[16] K. S. Paul Cichonski, Tom Millar, Tim Grance, ‘Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology’, *NIST Spec. Publ.*, vol. 800–61, p. 79, 2012.

[17] W. Wang and N. Lu, ‘Security risk analysis and security technology research of government public data center’, in *Proceedings - 2nd IEEE International Conference on Energy Internet, ICEI 2018*, 2018, pp. 185–189.

[18] W. Wang, Y. Shang, Y. He, Y. Li, and J. Liu, ‘BotMark: Automated botnet detection with hybrid analysis of flow-based and graph-based traffic behaviors’, *Inf. Sci. (Ny).*, vol. 511, pp. 284–296,

2020.

[19] A. Sharma, Z. Kalbarczyk, J. Barlow, and R. Iyer, ‘Analysis of security data from a large computing organization’, *Proc. Int. Conf. Dependable Syst. Networks*, pp. 506–517, 2011.

[20] J. Breier and J. Branišová, ‘A Dynamic Rule Creation Based Anomaly Detection Method for Identifying Security Breaches in Log Records’, *Wirel. Pers. Commun.*, vol. 94, no. 3, pp. 497–511, 2017.

[21] V. Minkevics and J. Kampars, ‘Methods, models and techniques to improve information system's security in large organizations’, *ICEIS 2020 - Proc. 22nd Int. Conf. Enterp. Inf. Syst.*, vol. 1, no. Iceis, pp. 632–639, 2020.

[22] M. Cinque, R. Della Corte, and A. Pecchia, ‘Contextual filtering and prioritization of computer application logs for security situational awareness’, *Futur. Gener. Comput. Syst.*, vol. 111, pp. 668–680, 2020.

[23] R. J. La, ‘Role of network topology in cybersecurity’, *Proc. IEEE Conf. Decis. Control*, vol. 2015-Febru, no. February, pp. 5290–5295, 2014.

[24] M. Trovati, W. Thomas, Q. Sun, and G. Kontonatsios, ‘Assessment of Security Threats via Network Topology Analysis: An Initial Investigation BT - Green, Pervasive, and Cloud Computing’, 2017, pp. 416–425.

[25] A. A. Daya, M. A. Salahuddin, N. Limam, and R. Boutaba, ‘BotChase: Graph-Based Bot Detection Using Machine Learning’, *IEEE Trans. Netw. Serv. Manag.*, vol. 17, no. 1, pp. 15–29, 2020.