RIGA TECHNICAL UNIVERSITY

Vladislavs Minkevičs

BIG DATA PARADIGM-BASED SOLUTIONS FOR IMPROVING INFORMATION SYSTEMS SECURITY MANAGEMENT

Summary of the Doctoral Thesis

RTU Press
Riga 2026

RIGA TECHNICAL UNIVERSITY
Faculty of Computer Science, Information Technology and Energy
Institute of Information Technology

Vladislavs Minkevičs

Doctoral Student of the Study Programme "Computer Science and Information Technology"

BIG DATA PARADIGM-BASED SOLUTIONS FOR IMPROVING INFORMATION SYSTEMS SECURITY MANAGEMENT

Summary of the Doctoral Thesis

Scientific supervisor

Associate Professor Dr. sc.ing.

JĀNIS KAMPARS

RTU Press

Riga 2026

Minkevičs, V. Big Data Paradigm-Based Solutions for Improving Information Systems Security Management. Summary of the Doctoral Thesis. – Riga: RTU Press, 2026. – 46 p.

Published in accordance with the decision of the Promotion Council "RTU P-07" of January 23 2026, Minutes No. 04030-9.7/1.

Cover image – AI generated from www.freepik.com.

https://doi.org/10.7250/9789934372919

ISBN 978-9934-37-291-9 (pdf)

DOCTORAL THESIS PROPOSED TO RIGA TECHNICAL UNIVERSITY FOR PROMOTION TO THE SCIENTIFIC DEGREE OF DOCTOR OF SCIENCE

To be granted the scientific degree of Doctor of Science (Ph. D.), the present Doctoral Thesis has been submitted for the defence at the open meeting of RTU Promotion Council on May 11, 2026 at 14.30 at the Faculty of Computer Science, Information Technology and Energy of Riga Technical University, Zundas krastmala street, Room 206.

OFFICIAL REVIEWERS

Associate professor *Dr. sc. ing.* Dmitrijs Bļizņuks,
Riga Technical University

Professor *Dr. sc. ing.* Gatis Vītols,
Latvia University of Life Sciences and Technologies, Latvia

Professor *Dr. sc.* Linas Bukauskas,
Vilnius University, Lithuania

DECLARATION OF ACADEMIC INTEGRITY

I hereby declare that the Doctoral Thesis submitted for review to Riga Technical University for promotion to the scientific degree of Doctor of Science (Ph. D.) is my own. I confirm that this Doctoral Thesis has not been submitted to any other university for promotion to a scientific degree.

Vladislavs Minkevičs ……. (signature)
Date: ……

The Doctoral Thesis has been written in Latvian/English. It consists of an Introduction; 4 Chapters; Conclusion; 49 figures; 32 tables; 1 appendice; the total number of pages is 171, including appendices. The Bibliography contains 140 titles.

ANNOTATION

The Thesis is devoted to solving a topical contemporary problem related to the mitigation of information systems security risks in an organisation. As a result, an adaptive security management model was developed, as well as a technological platform for mitigating security risks, which performs appropriate adaptations in response to incidents. The developed technological platform and the proposed set of modules combine many information sources and are based on the big data paradigm, ensuring adequate security of information systems, including meeting the requirements of both European and Latvian legislation in the field of cybersecurity. The developed solution has been tested at Riga Technical University (RTU) and has proven its effectiveness by improving the ability to respond to identified incidents and reducing the number of Latvian Information Technology Security Incident Response Team (CERT.LV) notifications about infected devices in the RTU network by 99.98 %, as well as increasing the ability to respond immediately to security incidents. Fast and automated involvement of the user of a potentially infected device using the offered technological platform ensured mitigation of security risks by implementation of preventive or corrective actions in a timely manner. The technological platform proposed in the work is scalable and based on open technologies and big data. The platform can be used in any organisation or institution that can provide access to audit trails and its network traffic, as the platform is based on the analysis of data from various sources, including intrusion detection, prevention systems, firewalls, network data, as well as any other data sources that are capable of creating audit trails. The platform collects and analyses the data received, and applies machine learning-based techniques to detect unknown threats by analysing both domain requests and network data. The platform reduces security risk by detecting and automatically responding to identified security risks in a variety of ways. In addition to RTU, the project was tested in the Procurement Monitoring Bureau and the Central Finance and Contracting Agency.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

EDR – Endpoint Detection and Response (used to detect if malware is installed on an endpoint device and to find ways to respond to this type of threat).

SIEM – Security Information and Event Management (used to provide a single central location to store and analyse data from different log sources).

SOC – Security Operations Centre (where the security of the network, servers and other systems is monitored using various tools and technologies to identify and prevent security threats).

ISMS – an adaptable security operations centre platform proposed in the Thesis, based on capability methodology.

IDS – Intrusion Detection System (aims to identify threats in network data in real time).

NetFlow – a solution implemented by CISCO with the aim of collecting and analysing network metadata.

CERT.LV – Cyber Incident Response Team, which aims to promote the security of information technologies in Latvia.

CDD – capability methodology for specifying and implementing adaptive solutions

DGA – algorithmically generated domains used by robot networks to communicate and pass necessary instructions.

SVC – supervised machine learning classifier for support vector machine.

NNC – supervised machine learning classifier neural networks that mimic biological processes in the brains of living organisms.

DTC – supervised machine learning classifier for decision trees, which is widely used for decision visualisation.

RFC – supervised machine learning classifier decision forests, which are a combination of decision trees.

MAC – the unique address of a device, which is assigned to it by the device manufacturer during the manufacturing process. The address contains both the manufacturer code and a unique device identifier.

General description of the Thesis

Topic relevance

In today's world, it is hard to imagine a sector that can exist without information technology. Both the public and private sectors are dependent on information technologies and, given the increasing digitalisation of the world, this dependence is growing and will continue to grow in the future [1]. Information and communication technologies are mainly used to make people's lives easier, through remote and secure financial transactions, communication with public authorities and other purposes. As dependence on information and communication technologies increases, so does the likelihood that they can be used to cause significant damage to public administration information systems and electronic communications networks, neutralise national political, economic and military decision-making centres, misinform the public and cause technogenic disasters. This increases the likelihood of non-military threats with severe consequences. For institutions responsible for the provision of state functions, the security of critical national information systems is of particular concern.

Both individual countries and the European Union as a whole have adopted laws, directives, and regulations governing information technology security, with one of the most recent initiatives being the NIS2 Directive [2]. These laws and regulations define minimum requirements for data protection in terms of confidentiality, integrity, and availability, which generally improve cybersecurity. Cybersecurity is the ability to protect networks, devices and data from unauthorised access or criminal use, and to ensure the confidentiality, integrity and availability of information [3]. Mitigating cybersecurity risks requires planning, implementation and monitoring of progress. However, cybersecurity incidents are rampant, for example, SolarWinds supply chain attack [4], the Colonial Pipeline ransomware incident [5], and denial-of-service attacks against Latvian state institutions [6]. These incidents are usually organised by well-funded criminal organisations, various criminal groups and even countries. Robot networks have become one of the biggest threats to cybersecurity today. According to the ENISA report for 2019–2020, more than 17 000 operating botnet servers have been identified [7].

Intrusion detection systems (IDSs) have been introduced to deal with cybersecurity threats. They have their origins in the US Air Force, where James P. Anderson developed a computer network threat monitoring system [8], which was able to continuously scan and compare network data against a known threat list. In the 1990s, IDS technologies were developed and were already capable of detecting network attacks, which were increasing in number and

complexity [9]. As IDS systems have evolved, many security companies have started to offer cloud-based solutions in which the only requirement for intrusion detection functionality is that the necessary data be uploaded to the cloud. However, such services are not very popular for one reason: the data sent to the cloud may contain personal data and sensitive business information. Another problem today is the shortage of cybersecurity specialists who can interpret the results of IDS and make decisions to improve security [10].

One of today's mistakes is to live in a false sense of security, believing that if no one writes anything negative about the organisation in the press, then everything must be fine. Organisations need to implement a set of preventive measures to protect both trade secrets and the private data of the organisation's employees from falling into the hands of unauthorised persons. As a first step, the author proposes appointing a person responsible for security management within the organisation. The person needs a wide range of tools to ensure security, as well as the appropriate knowledge of how to use them. It is necessary to monitor both the network and endpoint devices, to understand the configuration of the firewall and to assess potential sources of threats, including identifying vulnerabilities in devices and staying up-to-date with current information in the field of information and communication technologies.

Yakencheck Jason from securityintelligence.com [11] believes that manual actions are no longer sufficient to implement security management. A cybersecurity professional must be able to design and implement automated security monitoring tools, as well as have in-depth knowledge of computer networks, device architectures, vulnerabilities, cyber defences and their effectiveness.

The problem of security management requires taking into account the context of external data sources, various local measurements of information systems, and the objectives set by the company. The capability-driven development methodology helps to build systems that are informed by both context and business objectives, making it suitable for developing an IS security governance model.

According to [12], cybersecurity comprises five phases: identification (raising awareness of potential cyber risks), protection (implementing risk mitigation measures to protect critical resources), threat detection (applying tools to detect a cyber security incident), proactive threat response (taking actions to mitigate the impact of a cyber security incident), and incident recovery (a set of measures to keep services running after an incident).

The author concludes that the main challenge in companies and institutions is the threat detection and proactive action phases (Table 1).

Table 1

Cybersecurity Phases and the Solutions to Support Them

Cybersecurity phases	**Solutions**
Identification	CERT.LV [13]
Protection	NIS2 directive [2]
Threat identification	SIEM, SOC systems [14]–[19]
Proactive threat response	Level of awareness and knowledge of the person responsible for IS security (education, certification, practical skills)
Incident recovery	Continuous operations planning, NIS2 directive [2]

Similar problems have been encountered in every organisation where the author has assessed the compliance of security management with best practice, and the problem is particularly acute in higher education institutions, because usually very few resources are allocated to security management, and the study process is more concerned with increasing the speed and computing capacity of computer networks. These phases require continuous, full monitoring of the internal network, end devices and user activities on the network, as well as an understanding of how to identify a cybersecurity incident.

Aim and objectives of the Thesis

The aim of this Thesis is to develop a context-dependent, adaptive security management model and a technical implementation of this model within a security management platform that includes appropriate technical solutions to improve the cybersecurity environment.

The objective is based on the assumption that many organisations and institutions are unable to fully implement all five phases of cybersecurity according to [12].

To achieve the aim of the Thesis, the following tasks have been set.

1. Assess the current situation in the field of IS security management by conducting a literature review and research into the causes of cybersecurity incidents.

2. Identify existing research in the field of IS security management which uses both traditional threat identification tools and machine learning to identify unknown threats and to justify the need for building a technological platform.
3. Synthesise the requirements for a context-dependent adaptive security management model and its technical solutions.
4. Develop a context-dependent adaptive security management model.
5. Validate the defined model by designing an appropriate technical solution (platform) implementation in a higher education institution.
6. Evaluate the effectiveness of the developed model and platform.

Study methodology

The Thesis is based on the identification of problems in information systems security management and the proposal of solutions to these problems. In order to address the above problems, both qualitative and quantitative research methods were applied (Fig.1). Identifying and responding to threat levels according to different sources and using user feedback are defined as qualitative research methods in the study. The study defines the training of malicious activity modules and their identification algorithms as a quantitative research method. The primary data sources were data collected from the institution's internal network information, user workstations, switch data, firewall data, intrusion detection system data, NetFlow data, successful/failed authentication and other audit trail files and other data sources. Secondary data [20], [21] were used to train machine learning modules by classifying them as legitimate or malicious domains. Additional malicious domain names (secondary data) were extracted from the institution's firewall with intrusion prevention functionality, and the domain name request data and were explored, along with manual classification and comparison of suspicious domain name requests against malicious domain databases.

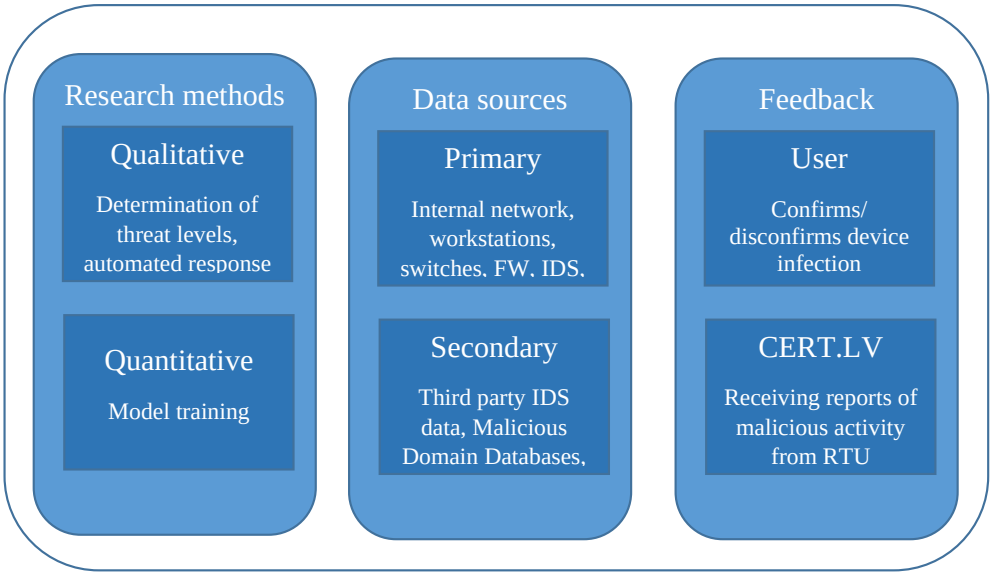

Fig.1. Research methodology.

To establish a feedback loop with information system users, forms were developed in Microsoft Office Forms to ask users of the potentially infected device whether they had scanned the device with recommended antiviruses and whether malicious code had been detected on the device. Additionally, CERT.LV notifications of malicious activity from the institution were also considered. In this way (by completed forms and CERT.LV reports), the accuracy of the trained machine learning models was increased by overtraining them.

The conceptual information security management capability model underlying adaptive information security management (ISM) was developed using the CDD [22] approach, as it is suitable for specifying and implementing adaptive solutions. The generic security management capability model was developed in the Thesis, as was the specific RTU-adapted capability model, both of which are based on modules that identify security risks and other elements for implementing security management.

The Thesis investigated machine learning-based models that identify malicious domains (DGAs). Experiments were conducted on selection criteria for DGA domains and on the construction of feature clusters. Different classifiers were chosen to identify DGAs: support vector machine (SVC), neural networks (NNC), decision trees (DTC) and random forests (RFC). To evaluate the performance of the classifiers, precision, accuracy, recall, and F1-score were measured for each classifier using cross-validation. The results of the experiments were compared with the results of the trained classifiers and the data from the firewall with IPS

functionality used in RTU. Experiments were also carried out with a machine learning-based NFAI module aimed at identifying malicious activity in network data.

The results of the DGA identification module were compared with the RTU firewall data. The results show that the effectiveness of ISMS improves when machine learning models are applied and when threats are identified at different levels by aggregating data from different modules. ISMS modules can also incorporate data from an organisation's cloud services that are not available to the firewall, further improving the identification of cybersecurity threats.

The study led to the definition of a context-dependent, adaptive security management model and the development of a corresponding big data-based, scalable security management system (ISMS) platform that can integrate independent threat detection and prevention modules according to the needs of the organisation. The ISMS platform is currently in active use at RTU to address cybersecurity threats.

Scientific contributions

1. Creation of a context-sensitive, adaptive IS security management model and its technical implementation.

2. Creation of training datasets for identifying malicious DNS as well as malicious code activity in network data.

3. Creation of a unique feature set for identifying a malicious DNS request, malicious code activity in network data.

4. Multidimensional threat aggregation algorithm’s development, which was integrated into the ISMS platform, providing a response based on the criticality of the identified threat.

5. Development of automated end-user involvement in cyber incidents, including end-user feedback.

Practical relevance of the work

Developed an IS security management model and its technical implementation, supporting the fulfilment of NIST-defined [12], introducing a threat identification and proactive phase. The platform has been implemented using mainly open-source solutions.

The platform has been validated at RTU. Multidimensional data analysis and aggregation based on the big data paradigm were applied, ensuring scalability of the platform. The platform is extensible with sub-modules according to the needs of the organisation. A machine learning-based domain identification module (DGA) has been validated at RTU and at other institutions, proving its effectiveness.

The effectiveness of the platform in securing information systems has been assessed.

Theses to be defended

Thesis 1. To ensure effective analysis of multi-dimensional data and identify security threats, it is necessary to apply big data technologies and machine learning techniques.

Thesis 2. The effectiveness of information systems security management depends on the ability to identify threats and the response time after threat identification.

Thesis 3. Security management requires the use of automated systems that respond to security threats.

Thesis hypothesis: Combining multiple data sources, specialised threat identification models, and platforms provides a more complete identification of security incidents compared to using individual dedicated solutions.

Approval of the Thesis results

The results were presented at twelve conferences

1. Riga Technical University 45th Scientific Conference, Riga (Latvia), 14–16 October 2004. Presentation “The search for effective risk management”.
2. 19th European Conference on Modelling and Simulation, Riga (Latvia), 1–4 June 2005. Presentation “Risk Management Modelling for Unified Threat Management Systems”.
3. 46th Scientific Conference of Riga Technical University, Riga (Latvia), 13–15 October 2005. Presentation “Risk management modelling using neural networks”.
4. 47th Scientific Conference of Riga Technical University, Riga (Latvia), 12–14 October 2006. Presentation “The use of real-time risk management in an organisation”
5. 6th Eurosim Congress "Eurosim 2007", Ljubljana (Slovenia), 9–13 September 2007. Presentation “Modelling a real-time risk management system”.
6. 48th Scientific Conference of Riga Technical University, Riga (Latvia), 11–13 October 2007. Presentation “The use of real-time risk management in the organisation”.
7. 48th Scientific Conference of Riga Technical University, Riga (Latvia), 13–15 October 2008. Presentation “Real-time risk management model”.
8. Modelling IT Security Risk Management in an Academic Environment. IEEE Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE'2017) 24 November 2017, Riga.
9. 59th International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS). IS Security Governance Capability Design for Higher Education Organisation. 12–14 November 2018, Riga.

10. ICEIS 2020 – 22nd International Conference on Enterprise Information Systems. Presentation “Methods, models and techniques to improve information systems’ security in large organisations”, 5–7 May 2020, Prague, Czech Republic, remotely.
11. 17th International Conference on Network and Service Management. Artificial intelligence and big data-driven IS security management solution with applications in higher education organisations. 25–29 October 2021, Izmir, Turkey.
12. IEEE Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE). Managing Information System Security in Higher Education Organisations. 27–29 April 2023, Vilnius, Lithuania.
13. Practical experience in creating a SOC using open source solutions, CERT.LV, 12 December 2023, online. https://cert.lv/lv/2023/11/it-drosibas-seminars-esi-dross-decembri.

The results of the research carried out in this Thesis have been presented in thirteen publications.

1. Minkevics, V., Slihte, J., Vulfs, G. “Search for effective risk management”, RTU Collection of Scientific Articles “Computer Science. Computer Control Technologies”, Vol. 5, No. 20, Riga, RTU, 2004, 174–180. (ISSN 1407-7493)
2. Minkevics, V., Slihte, J., Vulfs, G. “Modelling risk management for unified threat management systems”, 19th European Conference on Modelling and Simulation, Riga, 2005, 144–150. (ISBN 1-84233-112-4)
3. Minkevics, V., Slihte, J., Vulfs, G. “Modelling risk management system using neural networks”, RTU Collection of Scientific Articles “Computer Science. Computer Control Technologies”, Vol. 5, No. 23, Riga, RTU, 2005, 66–72. (ISSN 1407-7493)
4. Minkevics, V., Slihte, J., Vulfs, G. “Use of real – time risk management in organisation”, RTU Collection of Scientific Articles “Computer Science. Computer Control Technologies”, Vol. 5, No. 28, Riga, RTU, 2006, 23–29. (ISSN 1407-7493)
5. Minkevics, V., Slihte, J., Vulfs, G. “Modelling real-time risk management system”, Proceedings of the 6th EUROSIM Congress on Modelling and Simulation, Vol. 1, p. 414. (ISBN-13:978-3-901608-32-2)
6. Minkevics, V., Slihte, J., Vulfs, G. “Modelling real-time risk management system using associative approach”, RTU Collection of Scientific Articles “Computer Science. Computer Control Technologies”, Vol. 5, No. 31., Riga, RTU, 2007, 34–40. (ISSN 1407-7493)

7. Minkevics, V., Vulfs, G. “Real-time risk management model”, RTU Collection of Scientific Articles “Computer Science. Computer Control Technologies”, Vol. 36, Riga, RTU, 2008, 49–55. (ISSN 1407-7493)
8. Minkevičs, V., Šlihte, J. Modelling IT Security Risk Management in Academic Environment. In: 2017 5th IEEE Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE 2017): Proceedings, Latvia, Riga, 24–25 November 2017. Piscataway: IEEE, 2017, 5–8. ISBN 978-1-5386-4138-5. e-ISBN 978-1-5386-4137-8. Available: doi:10.1109/AIEEE.2017.8270562
9. Minkevičs, V., Kampars, J. IS Security Governance Capability Design for Higher Education Organisation. In: 2018 59th International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS 2018): Proceedings, Latvia, Riga, 29–29 November 2018. Piscataway: IEEE, 2018, 66–70. ISBN 978-1-7281-0099-9. e-ISBN 978-1-7281-0098-2. Available: doi:10.1109/ITMS.2018.8552975
10. Minkevičs, V., Kampars, J. Methods, models and techniques to improve information systems’ security in large organisations: included in registration. In Proceedings of the 22nd International Conference on Enterprise Information Systems. Vol. 1, 2020: ICEIS, 632-639, 2020, ISBN: 978-989-758-423-7
11. Minkevičs, V., Kampars, J., Artificial intelligence and big data-driven IS security management solution with applications in higher education organisations, 17th International Conference on Network and Service Management, 2021, Izmir, Turkey doi:10.23919/CNSM52442.2021.9615575
12. Minkevičs, V., Kampars, J., Grabis, J. Managing Information System Security in Higher Education Organisations, IEEE Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE), 27–29 April 2023. Vilnius, Lithuania. doi:10.1109/AIEEE58915.2023.10134911
13. Minkevičs, V., Grabis, J. A capability-driven automated cybersecurity monitoring and response system, Frontiers in Computer Science Journal, Vol. 7, 2025. doi:10.3389/fcomp.2025.1692263

Participation in RTU projects related to the work of the project.

1. Project: Perspective Technologies for Resilient and Secure Services (PPP-ARTSS: ARTSS, running from 1 July 2020 to 31 December 2020, https://artss.rtu.lv/).

2. Project: Development of a Big Data-driven ICT security management solution. Project duration from 1 January 2021 to 30 June 2023 (BICTSEMS, http://iti.rtu.lv/vitk/lv/petnieciba/projekti/lielo-datu-vadita-informacijas-un-komunikacijas-tehnologiju-drosibas).

Scope and structure

The Thesis consists of five chapters, Results and Conclusions, a list of references and two appendices.

Chapter 1 includes the basic concepts used in the Thesis, a literature review based on the Kofod-Petersen design science methodology [23], a description of the current situation and possible solutions.

Chapter 2 develops a solution to the problem by defining the basic requirements for the platform to be developed, including a high-level architecture for the technical solution. In this chapter, the platform to be developed is presented using the **c**apability approach [22].

Chapter 3 presents the implementation of the information systems security management platform at RTU, describes the components of the platform, and provides insight into the specifics of the platform, including architectural details for RTU use cases.

Chapter 4 evaluates the different modules included in the platform, such as the DGA module, which determines whether the name (domain) of the called website is typical or artificially generated. Artificially generated domains are used for communication between members of a malicious botnet. A threat aggregation module is also evaluated, which is based on combining the results of different modules in order to identify an infected device and reduce the number of false positives. The work evaluates the NFAI NetFlow network data analysis module, which uses a trained machine learning algorithm and, based on training data, determines whether a certain communication can be considered malicious or not.

Chapter 5 evaluates the ISMS platform in several steps and using different approaches, e.g., by comparing the platform with solutions available on the market, by measuring user responsiveness, and by evaluating individual modules of the platform.

The Results and Conclusions chapters present the results and conclusions of the research.

1. LITERATURE REVIEW AND POSSIBLE SOLUTIONS

The first chapter of the Thesis is a literature review in accordance with the principles of a structured literature review as defined in [23]. It is divided into three stages: planning, conducting and analysing the literature review. The research questions addressed in the literature review are summarised in Table 2.

Table 2

Overview of Issues Addressed in the Literature

Research question	Aim of the question	Expected result
What are the typical processes involved in information systems security management?	Identify the processes that make up IS security management	Description of IS security management processes
What data sources are used today to ensure the security of information systems (IS)?	Identify the sources of data used for security analysis and the methods used to process that data	List of data sources suitable for system security analysis and an overview of the methods used to process the data sources
What automated methods and tools are used for IS security management?	Identify which automation methods and tools are used today for IS security management	Overview of automation methods and their applications
What machine learning techniques are used for IS security management?	Identify what machine learning techniques and tools are used to identify unknown threats	Overview of different machine learning methods and tools used to identify unknown threats
What can be done to ensure automated stopping of malicious activity on the network?	Identify possible solutions to ensure automated stopping of malicious activity on the network	Description of solutions that can be used to instantly stop malicious activity on the network

The literature review [24]–[55] concludes that a complete security analysis requires the following:

1. NetFlow data, which can be obtained using various open source tools. This data allows the identification of network communication that deviates from “normal” network behaviour, thus identifying, for example, malicious code activity.

2. System audit trails, which can be used to identify atypical device behaviour by identifying malicious activity.

3. Honey pot functionality, which, by luring attackers, allows them to understand attack methods and possible tools, as well as providing additional time to protect real information systems in cases where an attacker has already penetrated the internal computer network.

4. Firewall data (audit trails), which accumulate information on incoming and outgoing traffic. This information can be used to determine whether firewall rules are functioning correctly and whether malicious activity has been detected on the network.

5. DNS data, which contains information on the source and destination IP address and port, as well as information on the requested DNS name. Domain name syntax can be analysed to identify algorithmically generated domain name requests, which in turn may indicate the presence of a device in the botnet.

The literature review concludes that IS security governance must involve the analysis of multidimensional data from a wide range of sources. There are also a large number of potentially applicable threat detection methods that would need to be implemented as independent threat identification services. The effective use of all available data sources and threat detection modules in a single security management solution that can be adapted to the organisational context is a problem that has not been sufficiently explored in the scientific literature and to which the author intends to pay particular attention by developing a context-dependent, adaptive security management model based on a capable methodology and its technical implementation, the ISMS platform.

2. CAPABILITY-DRIVEN SECURITY MANAGEMENT

Chapter 2 of the Thesis focuses on capability-oriented security management, which includes key concepts such as capabilities, contextual elements and measurable indicators. The capability-oriented security governance model developed in the Thesis is based on the capability-driven development (CDD) methodology [22]. It can take into account full contextual information, as well as perform automatic adaptive actions to restore the security level in the event of a threat.

A meta-model of the security governance model capability is defined in Fig. 2. The security governance model is characterised by objectives with measurable indicators, contextual elements that are measured using measurable properties, and a capability that adapts and uses both the contextual elements and the measurable properties.

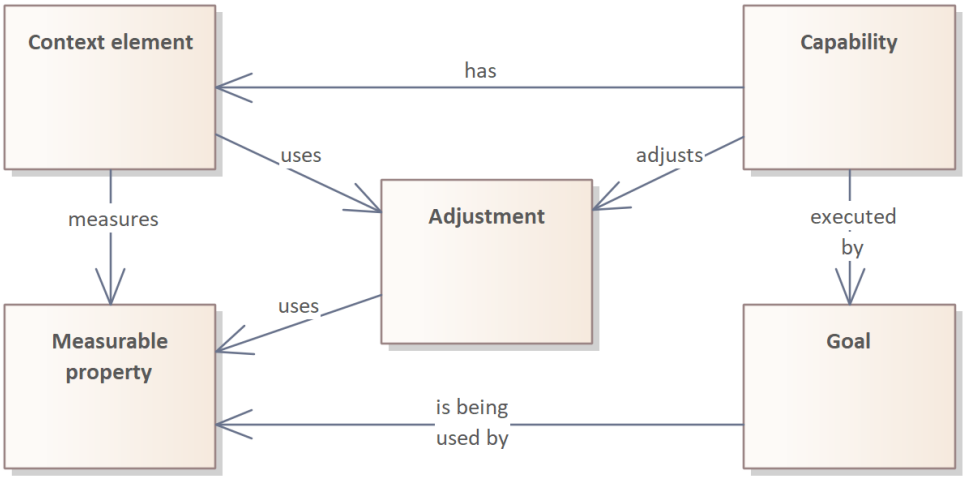

Fig. 2. Security management model capability meta-model.

Using the above approach, it is possible to describe the contextual elements, measurable indicators and capabilities of a security management system, thus clearly defining its operating principles.

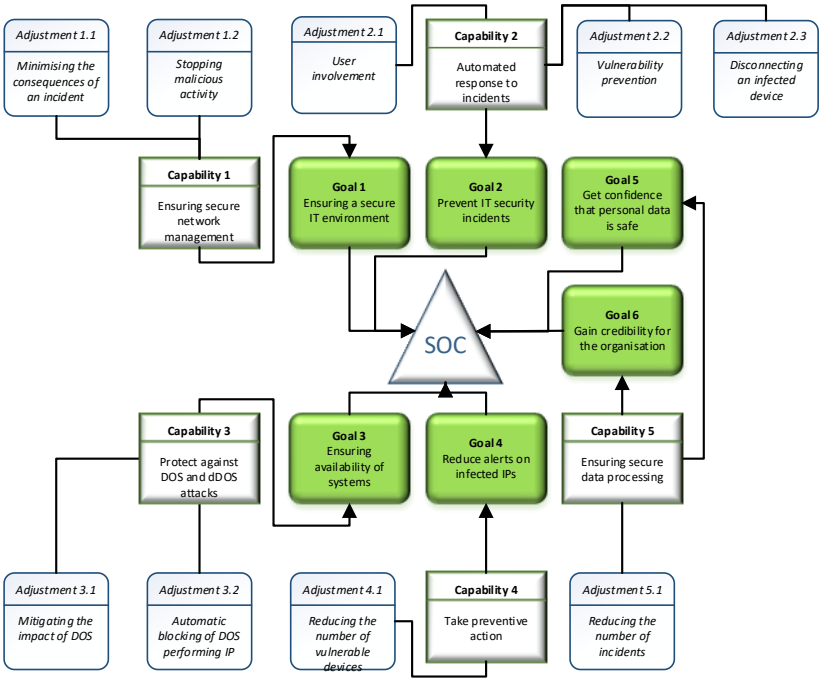

Fig. 3. General information security management capability.

Information security management capability (Fig. *3*) is implemented to achieve various objectives to improve security management. This capability fulfils the core Objective 1: Ensuring a secure IT environment, which is supported by five additional objectives.

Objective 2: Prevent IT security incidents.

Objective 3: Ensure availability of systems.

Objective 4: Reduce alerts on infected IPs.

Objective 5: Gain confidence that personal data is safe.

Objective: 6: Gain credibility for the organisation.

For each objective, there is a corresponding capability and adjustment.

Chapter 2 summarises the requirements for a technical solution (ISMS platform) to manage IS security according to the capability model defined in Table 3. It includes three key components: 1) data sources, 2) data analysis, and 3) action or response. The requirements for the ISMS platform are derived from the literature review and are applicable to any organisation

seeking to implement capability-based information security management. Table 3 outlines the anticipated outcomes associated with the implementation of each requirement.

Table 3

Specification of Requirements for the ISMS Platform

No.	Requirement
1.	Use open source technologies and high-level programming languages
2.	Ensure identification of the device and its network connection point, including scenarios involving dynamic IP address assignment
3.	Identify the user and involve them in the security management process
4.	Implement a scalable solution capable of handling larger volumes of data without requiring a complete rebuild of the platform
5.	Use open source-based intrusion detection with signature augmentation
6.	Use audit trail analysis to identify malicious activity
7.	Use an open-source-based network data analysis mechanism
8.	Use an open-source-based network metadata analysis mechanism
9.	Use the honeypot functionality to enable in-depth investigation of malicious code or human activity
10.	Identify theft of user authentication data
11.	Identify malicious network activity using network metadata and open source-based systems and machine learning
12.	Detect port scanning and password-guessing activities within the internal network
13.	Identify and temporarily block external IP addresses that are not involved in any communication – only port scanning
14.	Employ a threat-adaptive strategy that enables differentiated response times based on the nature and severity of specific threats
15.	Use automated identification of vulnerabilities and automatic reporting to the responsible party
16.	Identify algorithmically generated domains in DNS information using static lists and machine learning
17.	Disable devices that pose a threat to the internal network
18.	Display detected incidents and sent notifications to the person responsible for security using a graphical interface

The main components of the security management platform are shown in Fig. *4*. The platform components are implemented using technologies widely used in the open source industry, including Python3, Influx DB, Apache Kafka, and Grafana.

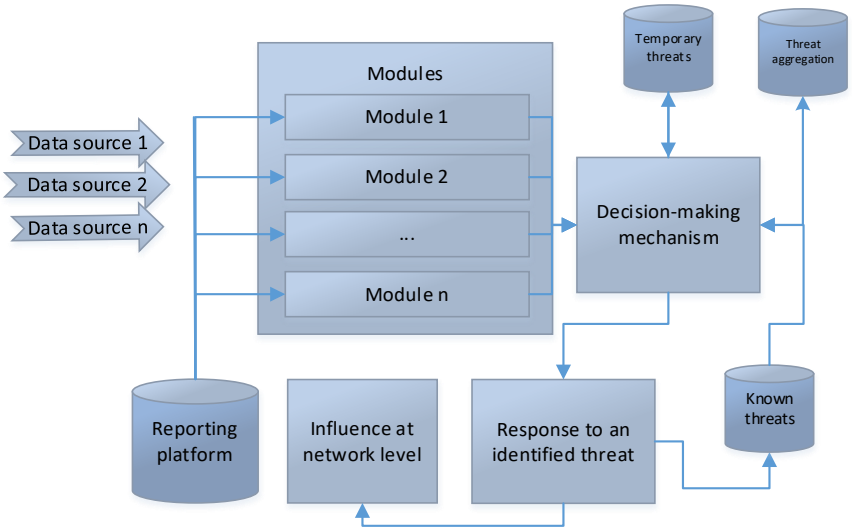

Fig. 4. Key components of the security management platform.

The framework of technologies used is expanded based on the information obtained during the modelling of the organisation's information security management capability. In this study, Apache Kafka and InfluxDB facilitated the integration of large-scale static and real-time data, while Apache Spark supported big data processing by enabling the detection of malicious activity within network traffic.

The main benefits of the proposed ISMS platform are:

- ensuring control of the final equipment;
- dynamic network data analysis;
- process automation;
- adaptive response;
- ability to add modules when attack vectors change;
- providing feedback, automated response and rapid implementation of system changes.

3. INTRODUCING A CAPABILITY-ORIENTED SECURITY MANAGEMENT MODEL AT THE RTU

In the third chapter, the general capability model (Fig. 3) is adapted for implementation at the Riga Technical University. Organisation-specific goals and their measurable properties are specified. In order to implement the requirements mentioned in the previous chapter, the organisation needs:

1) to ensure the ability to receive data from different data sources and understand network protocols;

2) to have knowledge of Python or another high-level scripting language to be able to adapt automation processes;

3) to know how to use open source software, including big data-based software;

4) to use static IP addresses on the internal network, or be able to identify dynamically assigned IP addresses using DHCP;

5) to know how to identify the end-user by IP address in order to be able to involve them in the mitigation of a security incident;

6) to know how to use open source or paid solutions to identify vulnerabilities;

7) to learn to use open source intrusion detection systems;

8) to know how to collect and use Netflow data;

9) to learn to use open source or paid honeypot solutions;

10) learn to work with M365 data, including Graph API;

11) to gain a comprehensive understanding of the API to effectively utilise it for both disconnecting devices from the network and for transmitting and receiving data between various information systems;

12) to know how to use firewall data;

13) to possess the capability to evaluate and prioritise security incidents based on the urgency of the required response;

14) to understand how DNS calls are made and be able to analyse them;

15) to know how to adjust the graphical interface of the security management system.

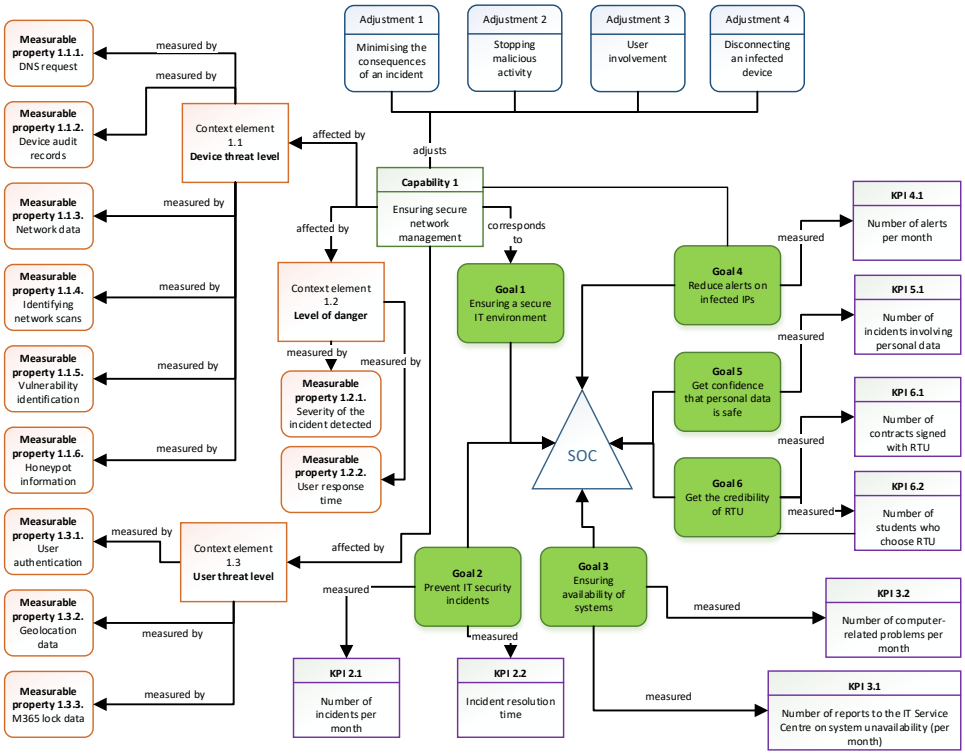

Fig. 5. Adjusted CDD target model.

In this model (Fig. 5), security management capability is specified to ensure the secure operation of the higher education institution. This capability fulfils Goal 1: Ensuring a secure IT environment, which is supported by five additional goals.

Goal 2: Prevent IT security incidents.

Goal 3: Ensuring the availability of systems.

Goal 4: Reduce alerts on infected IPs.

Goal 5: Gain confidence that personal data is safe.

Goal 6: Get the credibility of RTU.

Each sub-goal is measured by a different KPI to assess the achievement of that goal. Goal 2 is measured by KPI 2.1: Number of incidents per month, and KPI 2.2: Incident resolution time.

Goal 3 is measured by KPI 3.1: Number of reports to the IT Service Centre of system unavailability (per month), and KPI 3.2: Number of computer network-related problems per month. Goal 4 is measured by KPI 4.1: Number of alerts per month, and Goal 5 is measured by KPI 5.1: Number of incidents involving personal data. Finally, Goal 6 is measured by KPIs 6.1 and 6.2: Number of contracts signed with RTU and number of students who choose RTU for studies.

The capability is influenced by the relevant contextual elements: 1.1. Device threat level to identify whether a networked device is potentially infected and threatening other devices on the network; 1.2. Danger level to identify the response time to an incident; and 1.3. User threat level to understand whether a user has, for example, lost their authentication credentials. All contextual elements shall be assessed using a number of measurable properties. The device threat level is measured by 1.1.1. The DNS request, which determines whether the device is compromised by refraining from querying the botnet command centre domain to receive commands; 1.1.2. The device audit log (or log file data, if available); 1.1.3. Network traffic data, where atypical device behaviour is identified; 1.1.4. Network port scan identification; and 1.1.5. Vulnerability identification, where the device is tested for known vulnerabilities. The threat level or context element 1.2. Threat increases if the identified IT security incident is defined as high priority (critical) (metric 1.2.1) and if 1.2.2. User response time to the IT security incident is delayed. 1.3. The threat level of a user depends on the user authentication information recorded in the log files: 1.3.1. User authentication; 1.3.2. Geolocation data, which is used to identify the user's location during authentication, and 1.3.3. Microsoft 365 automated blocking mechanism that blocks users upon detection of spam activity. The user response rate is assessed by 1.2.2. User response time. Capability 1 is implemented through four primary services: a malicious activity identification service that uses multiple methods to identify infected devices on the network, an incident investigation service that ensures that the incident is accurately identified and its severity level determined, a user notification service that uses multiple means to inform users of the actions required to resolve the incident, and an infected device disabling service that uses firewalls and other devices to disable the infected device from the computer network. A detailed description of the elements of the capability model is provided in the Thesis and in the author’s publication [56]. The context and adaptation model is shown in Fig. 6.

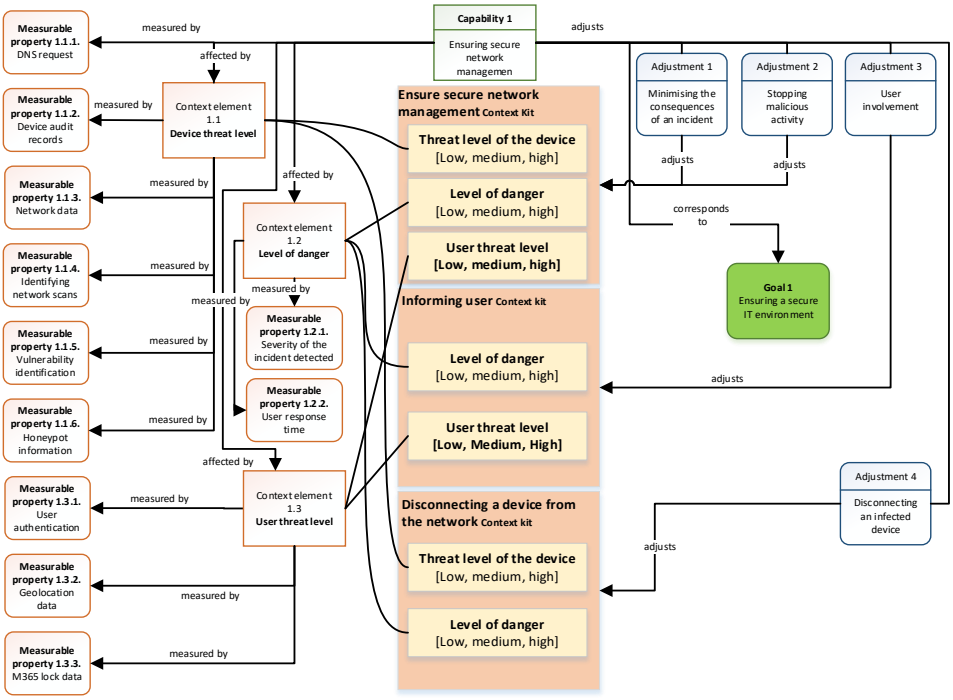

Fig. 6. Context and adaptation model.

For example, the adjustment “Make sure the message is not a false positive” determines the ability to identify false positives. The capability is provided by an expert-developed database with criteria for identifying true positives. For each of these criteria, a notification is formulated to be communicated to the user, outlining the necessary actions and instructions to mitigate the threat.

The adaptation of response capacity in the case of priority messages is shown in Fig. *7*. Depending on the number of reports of infected IPs and the number of incidents per month, the response to these incidents is further adjusted. If the number of reports exceeds a certain level, the priority of the reports is increased, and the previously used notification mechanism is changed from email to SMS.

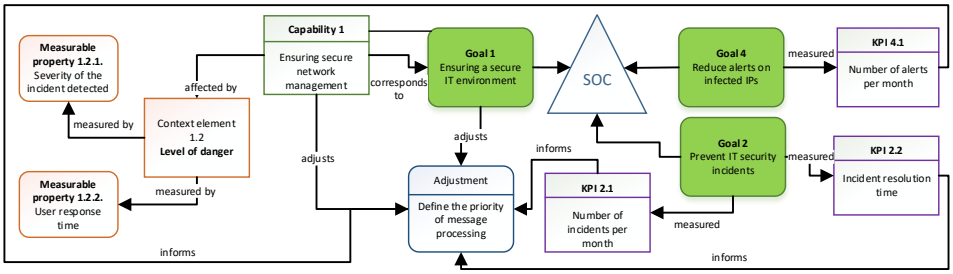

Fig. 7. Priority adjustment.

The ISMS platform includes (Fig. 8):

1. User Identification and Notification Module, which identifies the user whose device has been assigned an IP address. This module uses Apache Kafka [57] and Python scripts. The module includes 3 sub-modules:
    a. user notification via SMS;
    b. user notification via email;
    c. user notification via internal portal.
2. Administrator notification is provided via email and a graphical interface to the operations centre based on the Influx database [58] and Grafana graphical interface [59].
3. Access Blocking Module includes wireless network blocking using Aruba Clearpass [60]. Access to switches can be blocked automatically by microservices that pass information about the IP addresses to be blocked to the firewall.

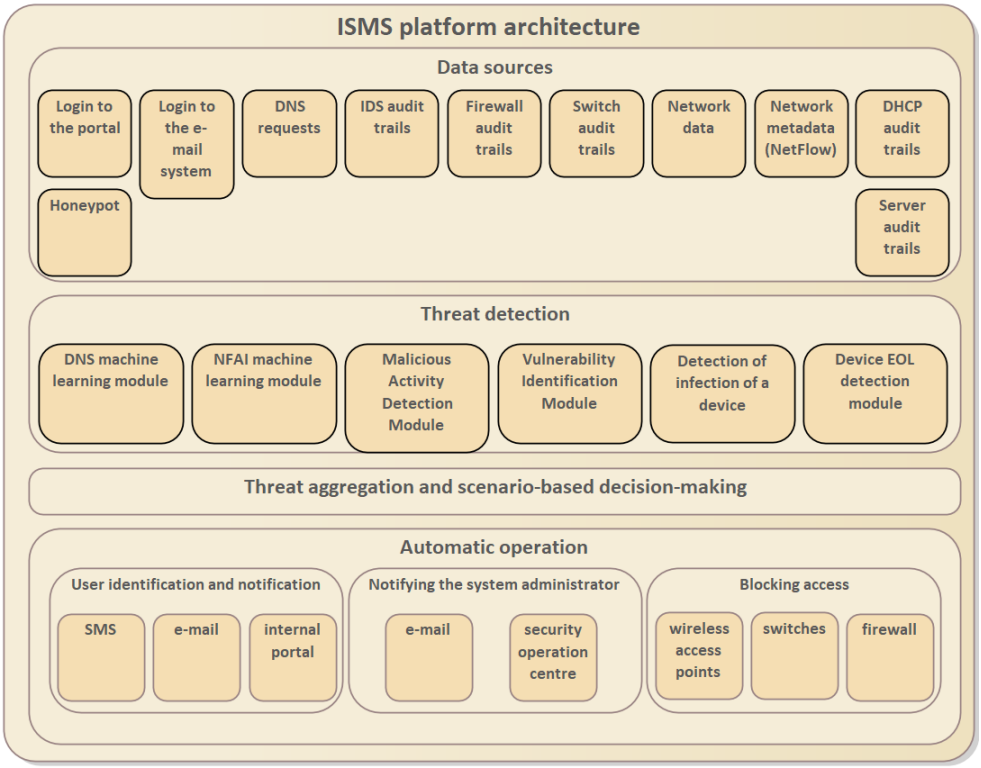

Fig. 8. ISMS platform architecture.

4. EVALUATION OF THE IS SECURITY MANAGEMENT PLATFORM

Chapter 4 assesses the model at various points in time, beginning in January 2021, employing diverse measurement methods. For the period from January 2021 to January 2024, the ISMS platform has generated more than 88 000 data points. Most of them were recommendations to scan the equipment and make security improvements, such as updating outdated software.

A DGA module has been evaluated to determine whether a DNS request can be classified as a DGA and thus be considered malicious. A set of features for training DNS classifiers was developed based on the study by Selvi et al. [39], using a set of 10 traits. The DGA module using the RFC machine learning algorithm was trained with 8856 “bad” and 8856 “good” domains and was compared with the Palo Alto firewall.

Table 4 compares the ML models, showing that RFC gave the best results.

Table 4

Comparison of the ML Models

Classificator	Precision	Recall	F1-score	Accuracy
RFC	0.934	0.948	0.941	0.940
DTC	0.916	0.928	0.922	0.921
NNC	0.869	0.854	0.862	0.852
SVM	0.858	0.860	0.859	0.859

The RFC model was refined by selecting the most appropriate features (Table 5).

Table 5

Comparison of the ML Models Based on Feature Sets

-	Precision	Recall	F1-score	Accuracy
Set 1	0.934	0.947	0.940	0.940
Set 2	0.933	0.946	0.939	0.939
Set 3	0.933	0.946	0.939	0.939
Set 4	0.930	0.946	0.938	0.938
Set 5	0.934	0.948	0.941	0.940

Table 5 demonstrates that the best results were obtained using the fifth set of features. More information on feature set selection can be found in the Thesis.

The DGA functionality of the Palo Alto firewall was compared with the DGA module. The DGA module, while possibly showing more false positives, has detected seven more DNS requests that are also considered DGA by a third party than the Palo Alto firewall (Table 6).

Table 6

Palo Alto Firewall Comparison to the DGA Module

No.		**DGA identified by firewall (total: 87)**	**DGA identified by module (total: 167)**
1.	Firewall identified DGA	87	25
2.	Module identified DGA	79	167
3.	Third-party identified DGA	31	18
4.	Third-party identified DGA, module identified DGA, but the firewall did not identify DGA	-	7

In addition to the DGA module, the NFAI module was evaluated to identify malicious activity in network data. Although the NFAI did not demonstrate strong performance, it remains a valuable supplementary tool for identifying malicious activity within the network.

This chapter also evaluates the threat aggregation module, which integrates the outputs of various modules to identify infected devices. The Influx DB database was used for this purpose. In order to perform threat aggregation, scenarios were developed that, when executed, generate a message of a certain priority. Depending on the priority of the message, the user of the device is notified, or the device is denied access to the network. Due to the dynamic issuance of IP addresses, the full functionality of the threat aggregation module requires binding the IP address to the MAC address of the device. During this binding process, the device's MAC address was treated as a unique identifier, and threat aggregation was conducted based on the criticality of the threats – for example, by designating a threshold number of medium-priority alerts to be classified as a threat. Threats can also be aggregated by threat category; e.g., if a DGA and other medium-priority messages are identified within a certain time interval, this is considered a threat.

Threat aggregation (Fig. *9*) was performed using different threat source sets, such as IDS audit logs, firewall data, and algorithmically generated domain names.

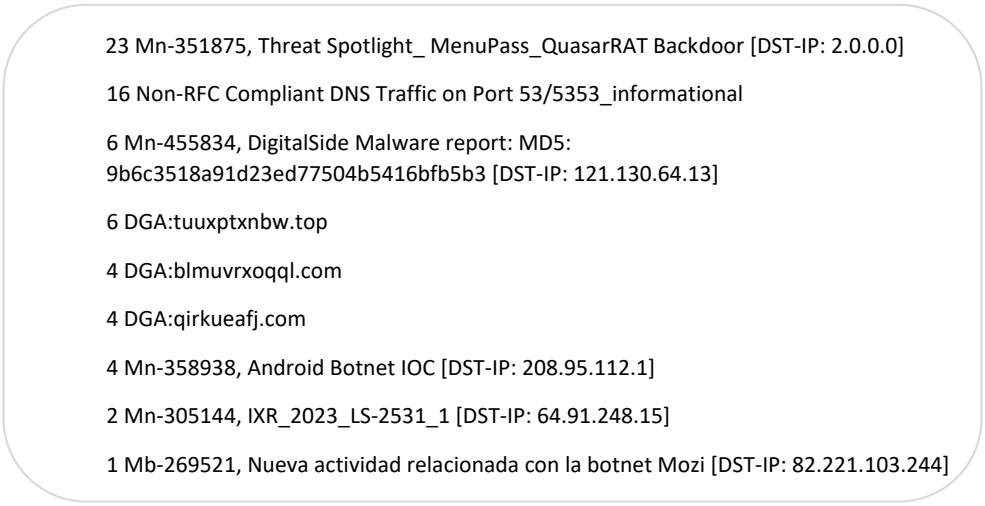

Fig. 9. Data aggregation using different threat source sets.

The main objective of the threat aggregation module is to reduce the number of false positives. Sometimes algorithmically generated domains are used to play targeted advertisements, so it would be wrong to immediately consider the invocation of such a domain a threat. Also, IP addresses on various blacklists should not always be considered a direct indication of a threat, as security companies often do not check whether the blacklisted IP address is dynamically assigned, and if it is, the next customer who receives that dynamic IP address will be considered a threat. The message generated by the threat aggregation module is treated as a standard notification of identified threats and is communicated to the device user via email. Additionally, this threat aggregation approach can be applied to platform-generated messages, thereby elevating the priority of aggregated threats.

The ISMS platform was evaluated in several stages using different approaches. The ISMS platform was evaluated by comparing it with solutions available on the market, measuring user responsiveness, and evaluating its individual modules (Table 7).

Table 7

Structure of the Evaluation

No.	Platform evaluation description
1.	Evaluation of RTU IP address and port scanner identification module
2.	Platform comparison with Palo Alto firewall built-in IDS functionality
3.	User response time when receiving an automated message from the platform
4.	Platform performance evaluation based on user feedback
5.	Platform performance evaluation based on third-party reports of infected devices in the RTU network
6.	Gartner Magic Quadrant top performers comparison with the ISMS platform

The response time of users to recommendations where information was sent only by email and included in the portal is around 5–10 hours from receipt of the message, whereas alerts where information was sent, including by SMS, are seen within 5 minutes (Fig. 10).

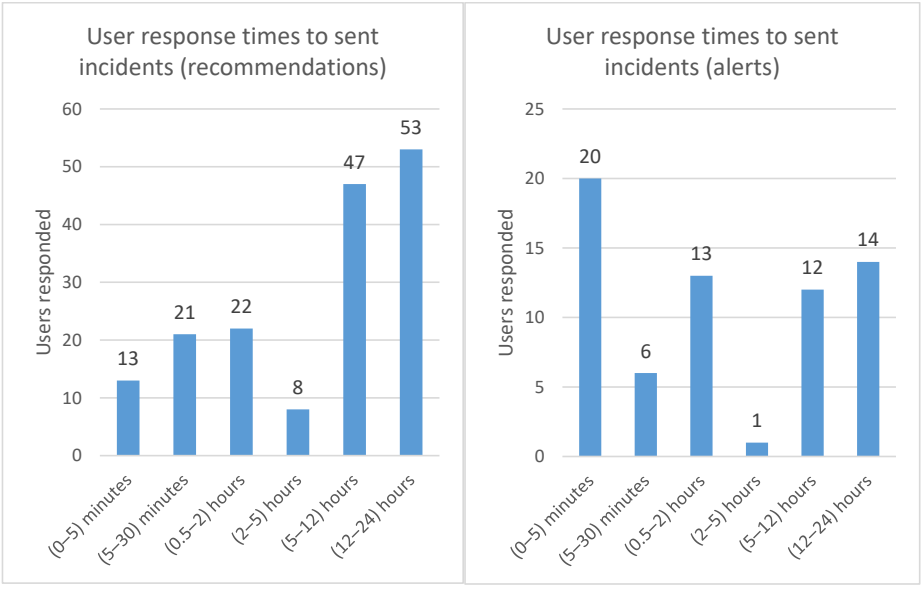

Fig. 10. Response time to warnings and recommendations.

The result suggests that the SMS notifications should be used in the case of severe incidents. However, it should not be overused to avoid messaging fatigue.

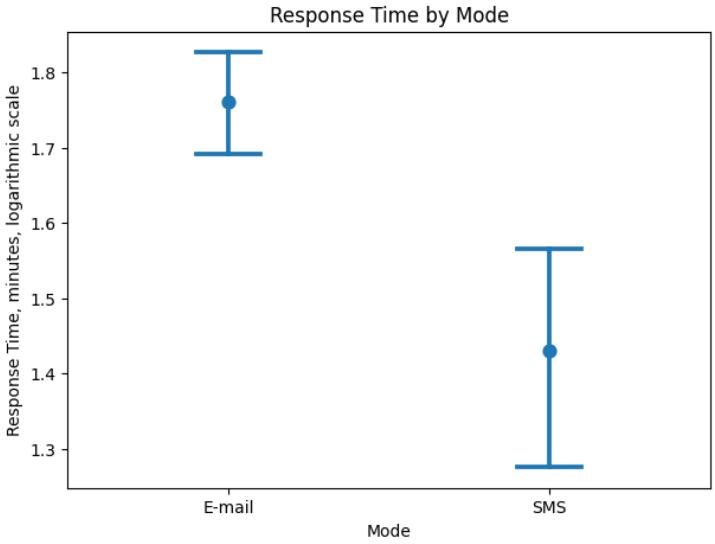

Fig. 11. The average response time according to the mode of communication.

The fact that the majority of users responded to the SMS notification within 5 minutes is confirmed in the interval plot showing the average response time according to the mode of communication (Fig. *11*). More detailed results of the evaluation of the other aspects are given in the Thesis.

RESULTS AND CONCLUSIONS

The primary objective of this Thesis was to develop a context-dependent adaptive security management model grounded in a capability-based methodology and supported by appropriate technical solutions. This model aims to enhance the cybersecurity environment by reducing the frequency of cybersecurity incidents and improving the speed of response to such events. In addition to achieving this main objective, an ISMS platform was developed, validated, and its performance evaluated. The following results were achieved:

1. An analysis and assessment of the current state of IS security management was performed.

2. Existing research was identified, and the capabilities of existing IS security management tools and services were explored.

3. The necessary controls that can be automated to ensure IS security management in the enterprise were identified.

4. The overall security management capability and high-level technical architecture for the ISMS platform were developed.

5. A capability model for the ISMS platform was developed, and the necessary modules to operate the ISMS platform were identified.

6) The implementation of the ISMS platform was defined.

7) The ISMS platform capability model was adapted to RTU requirements.

8) The performance of the ISMS platform was evaluated.

9) Conclusions and recommendations for the enhancement of information security management are presented.

The developed ISMS platform has been implemented at Riga Technical University since 2016, with the addition of various modules. In the beginning, it was just an IDS system with an automated option to notify the user about the identified infected device. Initially, it helped to reduce the number of CERT notifications about infected devices in the RTU network by more than half in the year following implementation. The situation further improved following the development of the technological solution (ISMS). The ability to automatically block a device whose user does not respond to notifications was introduced. Gradually, as additional ISMS platform modules were introduced, the number of CERT reports on infected devices in the RTU

network decreased. With the introduction of the Password theft identification module, it was found that the most frequent password thieves attempt to use legitimate user accounts to bypass the spam protection mechanism of the email server, and that the most frequent IP address range used by these miscreants is in Africa. Malicious actors continue to enhance their techniques, making phishing emails increasingly difficult to distinguish from legitimate correspondence. Additionally, HTML files are now commonly used as email attachments in such attacks. For instance, one of the most successful phishing campaigns observed by the author involved the use of a stolen user password, coupled with a previously sent email containing a reply link that purportedly shared a document. This link directed users to a counterfeit Microsoft 365 portal requiring authentication to access the document.

The integration of the DGA module into the ISMS platform facilitated the detection of botnet-infected devices, including a parking gate opener controller that had not been maintained since installation and subsequently became compromised. Although it is now possible to hide DNS using both DNS over HTTP and DNS over TLS methods, it has been observed that such methods are rarely used by malicious actors. The introduction of the DNS module helped to significantly reduce the number of CERT notifications, as many devices on the botnet behaved very cautiously and could only be identified via DNS requests. The study compared the DGA module with one of the best firewalls in the Gartner Quadrant [61], for which the manufacturer had provided DGA identification functionality. The DGA module identified the malicious request in 92.4 % of cases compared to the above firewall. The DGA module identified malware in 8.5 % of cases that was not detected by the firewall but was confirmed by at least one of three independent third-party sources ([62] and [63] or Quad9 [64]).

Although the NFAI module did not always work well, it did identify infected devices on the network, even when DNS request encryption was applied, as well as encryption of all traffic. According to user feedback, a total of 6 malware variants were identified that were not yet known to the firewall and the IDS system. The honeypot module has also produced positive results in identifying infected devices when they begin scanning network devices for new potential victims.

By combining different modules in the ISMS platform, the detection rate increased, and false alarms decreased.

By involving end-users in the incident response process and by being able to disable the device, the likelihood of an infected device infecting other devices on the network was reduced.

This is particularly relevant in cases where the infected device is not under RTU management (e.g. student devices).

Besides RTU, ISMS has also been implemented at two Latvian state institutions: Central Finance and Contracting Agency (CFCA) and the Procurement Monitoring Bureau (PMB). Table *8* summarises the key observations made on using ISMS at the aforementioned organisations. CFCA replaced the Splunk Security Information and Event Management (SIEM) system with ISMS, resulting in annual savings of approximately 50 000 EUR in licensing fees. These savings were primarily attributed to the elimination of Splunk license fees and reduced payments to external contractors responsible for configuring and monitoring Splunk events. Many third-party applications, such as a document management system at PMB, generate log files, which were separately analysed in these applications. The log file analysis was integrated into ISMS, reducing fees paid to third-party application developers and to the proprietary SIEM for handling additional data loads.

The value of these features has been confirmed by chief information officers at both organisations. ISMS was also presented to the Latvian information technology security community at the CERT.LV seminar "Be Secure" in 2023, as well as during the IT security event "Cyber Commando" held in Riga, Latvia, in 2024.

Table 8

ISMS Features Used at CFCA and PMB

Features	**CFCA**	**PMB**
Cost	Reduction of licensing fees	Parallel usage of ISMS and proprietary solutions
Data sources	The same set of data sources is used as for RTU	Additional data sources, such as logs from external enterprise systems, are added without increasing the licensing fee
Organisation-specific modules	Network traffic data analysis module for internal audit to monitor compliance	A module for analysing log files of the third-party applications using the ISMS services
Automated involvement of users	Institution-specific communication channels are integrated for distributing notifications	Instructions are sent out to users, and the users are nudged to resolve security concerns according to the instructions, while system administrators are involved in specific cases
Incident management	Notification types and notification triggers are tailored to the organisation's needs	Notification types and notification triggers are tailored to the organisation's needs

Finally, the author concludes that the ISMS platform is an equivalent solution to commercial products in the field of security management. The platform provides the identification and mitigation of cybersecurity risks required by an organisation and supports the author's hypothesis that combining multiple data sources, specialised threat identification models and platforms provides a more complete identification of security incidents compared to the use of individual dedicated solutions.

BIBLIOGRAPHY

[1] M. o. D. o. Latvia, " Latvian Cybersecurity strategy 2019-2022," 2019. [Online]. Available: http://tap.mk.gov.lv/doc/2018_11/AiMpamn_221118_PLKS.1220.docx. [Accessed 08.06.2020].

[2] "An official website of the European Union," 14.12.2022. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555. [Accessed 06.09.2023].

[3] CISA, "What is Cybersecurity?" Cybersecurity & Infrastructure Security Agency, 2009. [Online]. Available: https://us-cert.cisa.gov/ncas/tips/ST04-001. [Accessed 30.04.2021].

[4] "SolarWinds hack was 'largest and most sophisticated attack' ever," Reuters, 21.02.2021. [Online]. Available: https://www.reuters.com/article/us-cyber-solarwinds-microsoft-idUSKBN2AF03R. [Accessed 26.04.2021].

[5] "Colonial Pipeline CEO admits to authorizing $4.4 million ransomware payment," CNN, 19.05.2021. [Online]. Available: https://edition.cnn.com/2021/05/19/politics/colonial-pipeline-ransom/index.html. [Accessed 10.06.2021].

[6] "Nedēļas nogalē atvairīti kiberuzbrukumi 70 valsts iestāžu tīmekļa vietnēm," DIENA, [Online]. Available: https://www.diena.lv/raksts/latvija/zinas/nedelas-nogale-atvairiti-kiberuzbrukumi-70-valsts-iestazu-timekla-vietnem-14280778. [Accessed 24.05.2022].

[7] ENISA, "ENISA Threat Landscape 2020 – Botnet," ENISA, 20 10 2020. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-botnet. [Accessed 30.04.2021].

[8] J. P. Anderson, Computer Security Threat Monitoring and Surveillance, James P. Anderson Co., 1980.

[9] P. Scwab, "The History of Intrusion Detection Systems (IDS) – Part 1," 09.09.2015. [Online]. Available: https://www.threatstack.com/blog/the-history-of-intrusion-detection-systems-ids-part-1. [Accessed 08.06.2020].

[10] ISACA, "State of Cybersecurity 2020," ISACA, 2020. [Online]. Available: https://www.isaca.org/go/state-of-cybersecurity-2020. [Accessed 26.04.2021].

[11] J. Yakencheck, "Increase Automation to Overcome Cyber Resilience Challenges," [Online]. Available: https://securityintelligence.com/posts/increase-automation-to-overcome-cyber-resilience-challenges/. [Accessed 26.03.2020].

[12] N. I. o. S. a. Technology, "Framework for Improving Critical Infrastructure Cybersecurity," 18.04.2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. [Accessed 08.06.2020].

[13] "CERT.LV," [Online]. Available: https://cert.lv/lv. [Accessed 08.06.2021].

[14] "SOC-as-a-Service," Deltarisk, 2021. [Online]. Available: https://deltarisk.com/soc-as-a-service/. [Accessed 04.05.2021].

[15] R. Cybersecurity, "SOC as a Service," Radar Cybersecurity, 2021. [Online]. Available: https://www.radarcs.com/service-technology/managed-security-services/. [Accessed 04.05.2021].

[16] AT&T, "SOC as a service," AT&T, 2021. [Online]. Available: https://cybersecurity.att.com/solutions/security-operations-center/soc-as-a-service. [Accessed 04.05.2021].

[17] Profico, "SOC-as-a-Service," Profico, 2021. [Online]. Available: https://www.proficio.com/soc-as-a-service/. [Accessed 04.05.2021].

[18] Netsurion, "Security Operations Center (SOC)," Netsurion, 2021. [Online]. Available: https://www.netsurion.com/managed-threat-protection/security-operations-center. [Accessed 04.05.2021].

[19] "SOC Report Cost," TrustNet, 2021. [Online]. Available: https://www.trustnetinc.com/pricing/soc-ssae18-report-cost/. [Accessed 05.05.2021].

[20] "Alexa Top million domains," Alexa, [Online]. Available: http://s3.amazonaws.com/alexa-static/top-1m.csv.zip. [Accessed 11.08.2021].

[21] "Alexa Top Sites," Amazon, 2021. [Online]. Available: https://aws.amazon.com/alexa-top-sites/. [Accessed 07.05.2021].

[22] K. Sandkuhl and J. Stirna, Capability Management in Digital Enterprises, Springer International Publishing, 2018, p. 396.

[23] A. Kofod-Petersen, "How to do a Structured Literature Review in computer science," ResearchGate, 2015.

[24] M. Sheng, Machine Learning for Computer and Cyber Security Principles, Algorithms, and Practices, New York: CRC Press Taylor & Francis Group, 2019.

[25] M. A. F. B. S. OUIAZZANE, "A Multi-Agent Model for Network Intrusion Detection," in *2019 1st International Conference on Smart Systems and Data Science (ICSSD)*, 2019.

[26] S. C. M. M. a. D. C. A. Shah, "Building Multiclass Classification Baselines for Anomaly-based Network Intrusion Detection Systems," in *2020 IEEE 7th International Conference on Data Science and Advanced Analytics (DSAA)*, 759-760.

[27] S. S. Sivatha Sindhu, S. Geetha and A. Kannan, "Decision tree based light weight intrusion detection using a wrapper approach," *Expert Systems with Applications*, vol. 39, no. 1, pp. 129–141, 2012.

[28] Z. K. J. B. a. R. I. A. Sharma, "Analysis of security data from a large computing organization," in *IEEE/IFIP 41st International Conference on Dependable Systems & Networks (DSN)*, 506–517, 2011.

[29] N. F. A. G. E. M. a. M. P. I. Rose, "Something Is Better Than Everything: A Distributed Approach to Audit Log Anomaly Detection," in *IEEE Cybersecurity Development (SecDev)*, 2017.

[30] W. Z. a. W. Xinyu, "NetFlow Based Intrusion Detection System," in *2008 International Conference on MultiMedia and Information Technology*, 2008.

[31] K. Singh, S. C. Guntuku, A. Thakur, and C. Hota, *Big Data Analytics framework for Peer-to-Peer Botnet detection using Random Forests*, Information Sciences, 2014.

[32] B. B. Gupta, Machine Learning for Computer and Cyber Security Principles, Algorithms, and Practices, New York: CRC Press Taylor & Francis Group, 2018.

[33] R. D. C. A. P. Marcello Cinque, "Contextual filtering and prioritization of computer application logs for security situational awareness," *Future Generation Computer Systems*, vol. 111, ISSN 0167-739X, pp. 668–680, 2020.

[34] R. D. Muhammet Baykara, "A novel honeypot-based security approach for real-time intrusion detection and prevention systems," *Journal of Information Security and Applications*, vol. 41, pp. 103–116, 2018.

[35] S. K. Hajar Esmaeil As-Suhbani, "Classification of Firewall Logs Using Supervised Machine Learning Algorithms," in *International Journal of Computer Sciences and Engineering*, vol. 7, no. 8, 2019.

[36] F. F. Daniel Plohmann, U. o. B. Khaled Yakdan, D. Michael Klatt, J. Bader, and F. F. Elmar Gerhards-Padilla, "A Comprehensive Measurement Study of Domain Generating Malware," in *25th USENIX Security Symposium*, Austin, TX, 2016.

[37] A. Ahluwalia, I. Traore, K. Ganame, and N. Agarwal, "Detecting Broad Length Algorithmically Generated Domains," *Intelligent, Secure, and Dependable Systems in Distributed and Cloud Environments*, pp. 19–34, 2017.

[38] D.-T. Truong and G. Cheng, "Detecting domain-flux botnet based on DNS traffic features in managed network," *Security and Communication Networks*, vol. 9, no. 14, pp. 2338–2347, 2016.

[39] E.-O. Jose Selvi, Ricardo J.Rodríguez, "Detection of algorithmically generated malicious domain names using masked N-grams," *Elsevier*, vol. 124, pp. 156–163, 2019.

[40] H. S. A. A. A. D. G. Jonathan Woodbridge, *Predicting Domain Generation Algorithms with Long Short-Term Memory Networks*, Arlington,VA 22201: Endgame, Inc, 2016, p. 13.

[41] K. R. S. Barbosa, E. Souto, E. Feitosa, and K. El-Khatib, "Identifying and Classifying Suspicious Network Behavior Using Passive DNS Analysis," *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*, pp. 160–167, 2015.

[42] M. Mowbray and J. Hagen, "Finding Domain-Generation Algorithms by Looking at Length Distribution," in *2014 IEEE International Symposium on Software Reliability Engineering Workshops*, 2014.

[43] J. Peck, C. Nie, R. Sivaguru, C. Grumer, F. Olumofin, B. Yu, A. Nascimento, and M. D. Cock, "CharBot: A Simple and Effective Method for Evading DGA Classifiers," *IEEE Access*, pp. 91759–91771, 2019.

[44] J. Y. P. L. a. R. F. E. C. Zhong, "Learning From Experts' Experience: Toward Automated Cyber Security Data Triage", *IEEE Systems Journal*, vol. 13, pp. 603–614, 2019.

[45] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, and M. Xu, "A Survey on Machine Learning Techniques for Cyber Security in the Last Decade," *IEEE Access*, vol. 8, pp. 222310–222354, 2020.

[46] G. F. T. H. S. N. W.-S. Y. Jared Lee Lewis, "IP Reputation Analysis of Public Databases and Machine Learning Techniques," in *International Conference on Computing, Networking and Communications, ICNC 2020. IEEE*, 2020.

[47] F. a. M. J. P. Magalhaes, "Adopting machine learning to support the detection of malicious domain names," *7th International Conference on Internet of Things: Systems, Management and Security, IOTSMS 2020*, 2020.

[48] J. Y. Z. W. H. L. X. Sun, "HGDom: Heterogeneous Graph Convolutional Networks for Malicious Domain Detection," in *NOMS 2020 – 2020 IEEE/IFIP Network Operations and Management Symposium*, 2020.

[49] H. B. S. Nõmm, "Unsupervised Anomaly Based Botnet Detection in IoT Networks," in *17th IEEE International Conference on Machine Learning and Applications (ICMLA)*, 2018.

[50] Z. T. R. Z. L. L. J. Liu, "A Distance-Based Method for Building an Encrypted Malware Traffic Identification Framework," in *IEEE Access*.

[51] Z. Chkirbene, S. Eltanbouly, M. Bashendy, N. Alnaimi, and A. Erbad, "Hybrid Machine Learning for Network Anomaly Intrusion Detection," *IEEE International Conference on Informatics, IoT, and Enabling Technologies, ICIoT 2020*, pp. 163–170, 2020.

[52] R. M. Elbasiony, E. A. Sallam, T. E. Eltobely, and M. M. Fahmy, "A hybrid network intrusion detection framework based on random forests and weighted k-means," *Ain Shams Engineering Journal*, vol. 4, pp. 753–762, 2013.

[53] S. H. Mousavi, M. Khansari, and R. Rahmani, "A fully scalable big data framework for Botnet detection based on network traffic analysis," *Information Sciences*, no. 512, pp. 629–640, 2020.

[54] R. Alguliyev and Y. Imamverdiyev, "Big Data: Big Promises for Information Security," in *2014 IEEE 8th International Conference on Application of Information and Communication Technologies (AICT)*, 2014.

[55] M. D. H. Garg, "Securing IoT Devices and Securely Connecting the Dots Using REST API and Middleware," in *2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*, 2019.

[56] K. J. G. J. Minkevičs V., "Managing Information System Security in Higher Education Organizations," in *IEEE Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE)*, Vilnius, Lithuania, 2023.

[57] "Apache Kafka," Apache, 2021. [Online]. Available: https://kafka.apache.org/. [Accessed 06.05.2021].

[58] "Build on InfluxDB," InfluxData, 2021. [Online]. Available: https://www.influxdata.com/. [Accessed 06.05.2021].

[59] "Your observability wherever you need it," GrafanaLabs, 2021. [Online]. Available: https://grafana.com/. [Accessed 06.05.2021].

[60] "Secure Network Access Control for Modern IT," Aruba, 2021. [Online]. Available: Secure Network Access Control for Modern IT. [Accessed 06.05.2021].

[61] "Gartner Magic Quadrant," Gartner, [Online]. Available: https://www.gartner.com/en/research/methodologies/magic-quadrants-research. [Accessed 04.06.2021].

[62] "Introducing 1.1.1.1 for Families," Cloudfare, [Online]. Available: https://blog.cloudflare.com/introducing-1-1-1-1-for-families/. [Accessed 07.06.2021].

[63] "Norton ConnectSafe," Norton, [Online]. Available: https://en.wikipedia.org/wiki/Norton_ConnectSafe. [Accessed 07.06.2021].

[64] "An open DNS recursive service for free security and high privacy," Quad9, 2021. [Online]. Available: https://quad9.com/. [Accessed 07.05.2021].

[65] "Suricata Open Source IDS / IPS / NSM engine," The Open Information Security Foundation, [Online]. Available: https://suricata-ids.org/. [Accessed 20.08.2019].

[66] PWC, "24th Annual Global CEO Survey," PricewaterhouseCoopers, 2021. [Online]. Available: https://www.pwc.com/gx/en/ceo-agenda/ceosurvey/2021.html. [Accessed 26.04.2021].

[67] e. planet, "Top Cybersecurity Companies," eSecurity planet, 05.01.2021. [Online]. Available: https://www.esecurityplanet.com/products/top-cybersecurity-companies/. [Accessed 27.04.2021].

[68] ISO, "Information security management (ISO/IEC 27001)," ISO, 2013. [Online]. Available: https://www.iso.org/isoiec-27001-information-security.html. [Accessed 27.04.2021].

[69] CISA, "Cybersecurity Framework," CISA, 2021. [Online]. Available: https://us-cert.cisa.gov/resources/cybersecurity-framework. [Accessed 27.04.2021].

[70] Saeima, "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām," Saeima, 28 07 2015. [Online]. Available: https://likumi.lv/ta/id/275671-kartiba-kada-tiek-nodrosinata-informacijas-un-komunikacijas-tehnologiju-sistemu-atbilstiba-minimalajam-drosibas-prasibam. [Accessed 27.04.2021].

[71] E. P. U. PADOME, *EIROPAS PARLAMENTA UN PADOMES REGULA (ES) 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula),* Eiropas Savienības Oficiālais Vēstnesis, 2016.

[72] "Marriott reveals its second customer data breach in two years," CBSnews, 31 03 2020. [Online]. Available: https://www.cbsnews.com/news/marriott-data-breach-2020-5-million/. [Accessed 27.04.2021].

[73] "ICO fines Marriott International Inc," Information Commisioner's Office, 30.10.2020. [Online]. Available: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-marriott-international-inc-184million-for-failing-to-keep-customers-personal-data-secure/. [Accessed 27.04.2021].

[74] ""City Bee" pēc Lietuvas klientu datu noplūdes apgalvo, ka lietotāju dati Latvijā ir drošībā," Apollo ziņas, 17 02 2021. [Online]. Available: https://www.apollo.lv/7182586/city-bee-pec-lietuvas-klientu-datu-nopludes-apgalvo-ka-lietotaju-dati-latvija-ir-drosiba. [Accessed 27.04.2021].

[75] "Latvijā, iespējams, notikusi nekustamo īpašumu apsaimniekošanas uzņēmumu klientu datu noplūde," Ziņu aģentūra LETA, 05.02.2021. [Online]. Available: https://nra.lv/latvija/338501-latvija-iespejams-notikusi-nekustamo-ipasumu-apsaimniekosanas-uznemumu-klientu-datu-noplude.htm. [Accessed 27.04.2021].

[76] C. I. f. Cybersecurity, "Publiski pieejams datu avots NSL-KDD," 2009. [Online]. Available: https://www.unb.ca/cic/datasets/nsl.html. [Accessed 30.04.2021].

[77] MITRE, "Risk Mitigation Planning, Implementation, and Progress Monitoring," MITRE Corporation, 2018. [Online]. Available: https://www.mitre.org/publications/systems-engineering-guide/acquisition-systems-engineering/risk-management/risk-mitigation-planning-implementation-and-progress-monitoring. [Accessed 03.05.2021].

[78] "Firefox DNS-over-HTTPS," Firefox, [Online]. Available: https://support.mozilla.org/en-US/kb/firefox-dns-over-https. [Accessed 03.05.2021].

[79] M. Vale, "Google Public DNS now supports DNS-over-TLS," Google, 2019. [Online]. Available: https://security.googleblog.com/2019/01/google-public-dns-now-supports-dns-over.html. [Accessed 03.05.2021].

[80] Cloudflare, "DNS over TLS," Cloudflare, 2021. [Online]. Available: https://developers.cloudflare.com/1.1.1.1/dns-over-tls. [Accessed 03.05.2021].

[81] Zonefiles, "Compromised domain list," Zonefiles, 05.2021. [Online]. Available: https://zonefiles.io/compromised-domain-list/. [Accessed 03.05.2021].

[82] McAfee, "10 key functions performed by the SOC," McAfee, 2021. [Online]. Available: https://www.mcafee.com/enterprise/en-us/security-awareness/operations/what-is-soc.html#definition. [Accessed 03.05.2021].

[83] M. R. Long, "A Small Business Guide to the Security Operations Center," Montley Fool, 18.11.2020. [Online]. Available: https://www.fool.com/the-blueprint/soc/. [Accessed 04.05.2021].

[84] Y. Korff, "How much does it cost to build a 24x7 SOC?" 28.02.2018. [Online]. Available: https://expel.io/blog/how-much-does-it-cost-to-build-a-24x7-soc/. [Accessed 05.05.2021].

[85] "Intelligent Management Software," Hewlett Packard Enterprise, 2021. [Online]. Available: https://buy.hpe.com/us/en/software/intelligent-management-software/c/c001014. [Accessed 05.05.2021].

[86] "The Nessus Family," Tenable, 2021. [Online]. Available: https://www.tenable.com/products/nessus. [Accessed 05.05.2021].

[87] "Downloading Nmap," Nmap.org, 2021. [Online]. Available: https://nmap.org/download.html. [Accessed 05.05.20201].

[88] "Apache Spark™ is a unified analytics engine for large-scale data processing.," Apache, 2021. [Online]. Available: https://spark.apache.org/. [Accessed 06.05.2021].

[89] P. H. Z. Hu, L. Zhu, J. Heidemann, A. Mankin, D. Wessels, *Specification for DNS over Transport Layer Security (TLS)*, IETF Tools, 2016, p. 18.

[90] Mozilla.org, "About DNS-over-HTTPS," Mozilla.org, 07 01 2020. [Online]. Available: https://support.mozilla.org/en-US/kb/firefox-dns-over-https#w_about-dns-over-https. [Accessed 07.01.2020].

[91] "Analyze suspicious files and URLs to detect types of malware," VirusTotal, 2021. [Online]. Available: https://www.virustotal.com/gui/home/url. [Accessed 07.05.2021].

[92] "ICANN root zone," ICANN, 2021. [Online]. Available: http://stats.research.icann.org/dns/tld_report/archive/index.html. [Accessed 07.05.2021].

[93] "fprobe," SourceForge, 2016. [Online]. Available: https://sourceforge.net/p/fprobe/wiki/Home/. [Accessed 13.05.2021].

[94] "nfdump," GitHub, 2021. [Online]. Available: https://github.com/phaag/nfdump. [Accessed 13.05.2021].

[95] K. P. Shung, "Accuracy, Precision, Recall or F1?" 15.05.2015. [Online]. Available: https://towardsdatascience.com/accuracy-precision-recall-or-f1-331fb37c5cb9. [Accessed 25.03.2021].

[96] F. Pacheco, E. Exposito, M. Gineste, C. Baudoin, and J. Aguilar, "Towards the Deployment of Machine Learning Solutions in Network Traffic Classification: A Systematic Survey," 2019.

[97] "BlackBerry Protect," BlackBerry, [Online]. Available: https://www.blackberry.com/us/en/products/unified-endpoint-security/blackberry-protect. [Accessed 10.06.2021].

[98] "McAfee Endpoint Security," McAfee, [Online]. Available: https://www.mcafee.com/enterprise/en-us/products/endpoint-security.html. [Accessed 10.06.2021].

[99] "Prevent endpoint breaches," Broadcom, [Online]. Available: https://www.broadcom.com/products/cyber-security/endpoint/end-user. [Accessed 10.06.2021].

[100] D.-b. X. Lin Li, "Research on the network security management based on data mining," in *2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)*, Chengdu, China, 2010.

[101] "Blacklist Check List," [Online]. Available: https://whatismyipaddress.com/blacklist-check. [Accessed 16.06.2021].

[102] "Blacklists," [Online]. Available: https://mxtoolbox.com/blacklists.aspx. [Accessed 16.06.2021].

[103] "IPv4 – Packet Structure," TutorialsPoint, [Online]. Available: https://www.tutorialspoint.com/ipv4/ipv4_packet_structure.htm. [Accessed 16.06.2021].

[104] "Suricata User Guide," Suricata, [Online]. Available: https://suricata.readthedocs.io/en/suricata-6.0.2/. [Accessed 16.06.2021].

[105] R. Gerhards, *The Syslog Protocol.*

[106] "The World's First Truly Open Threat Intelligence Community," Aleanvault, [Online]. Available: https://otx.alienvault.com/. [Accessed 18.06.2021].

[107] "IBM Security QRadar," IBM, [Online]. Available: https://www.ibm.com/security/security-intelligence/qradar. [Accessed 18.06.2021].

[108] "Security Information and Event Management (SIEM)," Logrhythm, [Online]. Available: https://logrhythm.com/solutions/security/siem/. [Accessed 18.06.2021].

[109] "Splunk Enterprise Security," Splunk, [Online]. Available: https://www.splunk.com/en_us/software/enterprise-security.html. [Accessed 18.06.2021].

[110] "The Significance and Role of Firewall Logs," Exabeam, [Online]. Available: https://www.exabeam.com/siem-guide/siem-concepts/firewall-logs/. [Accessed 09.08.2021].

[111] D. W. V. a. J. P. Sharma, "Optimized Classification of Firewall Log Data using Heterogeneous Ensemble Techniques," in *2021 International Conference on Advanced Computing and Innovative Technologies in Engineering, ICACITE 2021*, 2021.

[112] "Intrusion detection system," Wikipedia, [Online]. Available: https://en.wikipedia.org/wiki/Intrusion_detection_system. [Accessed 10.08.2021].

[113] "AbuseIPDB," [Online]. Available: https://www.abuseipdb.com/. [Accessed 11.08.2021].

[114] "DGA Collection," [Online]. Available: https://github.com/pchaigno/dga-collection. [Accessed 11.08.2021].

[115] abuse.ch, [Online]. Available: https://urlhaus.abuse.ch/downloads/text/. [Accessed 11.08.2021].

[116] "English Dictionary," Cambridge, [Online]. Available: https://dictionary.cambridge.org/dictionary/english/. [Accessed 11.08.2021].

[117] "Vulnerabilities, Exploits, and Threats at a Glance," Rapid7, [Online]. Available: https://www.rapid7.com/fundamentals/vulnerabilities-exploits-threats/. [Accessed 11.08.2021].

[118] "The OWASP Testing Project," OWASP, [Online]. Available: https://owasp.org/www-project-web-security-testing-guide/latest/2-Introduction/README. [Accessed 11.08.2021].

[119] "CVE details," MITRE Corporation, [Online]. Available: https://www.cvedetails.com/index.php. [Accessed 11.08.2021].

[120] "OpenVas by Greenbone," Greenbone, [Online]. Available: https://openvas.org. [Accessed 11.08.2021].

[121] "One platform, one agent, one view," Qualys, [Online]. Available: https://www.qualys.com. [Accessed 11.08.2021].

[122] "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām," likumi.lv, [Online]. Available: https://likumi.lv/ta/id/275671-kartiba-

kada-tiek-nodrosinata-informacijas-un-komunikacijas-tehnologiju-sistemu-atbilstiba-minimalajam-drosibas-prasibam. [Accessed 12.08.2021].

[123] API Explorer, "API Explorer," Aruba, [Online]. Available: https://www.arubanetworks.com/techdocs/ClearPass/6.7/Guest/Content/AdministrationTasks1/API_Explorer.htm. [Accessed 12.08.2021].

[124] "clearpass-api-python," Aruba, [Online]. Available: https://github.com/aruba/clearpass-api-python. [Accessed 12.08.2021].

[125] "Getting started with the REST API," Hewlett Packard, [Online]. Available: https://developers.hp.com/hp-proactive-management/getting-started-rest-api. [Accessed 12.08.2021].

[126] "REST API Guide," Juniper, [Online]. Available: https://www.juniper.net/documentation/us/en/software/junos/rest-api/index.html. [Accessed 12.08.2021].

[127] "PAN-OS REST API," Palo Alto, [Online]. Available: https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-panorama-api/get-started-with-the-pan-os-rest-api/pan-os-rest-api.html. [Accessed 12.08.2021].

[128] Y. S. Y. H. Y. L. J. L. Wei Wang, "BotMark: Automated botnet detection with hybrid analysis of flow-based and graph-based traffic behaviors," *Information Sciences*, vol. 511, pp. 284–296, 2020.

[129] E. S. I. K. I. S. A. Privalov, "Graph-based evaluation of probability of disclosing the network structure by targeted attacks," in *NOMS 2020 – 2020 IEEE/IFIP Network Operations and Management Symposium*, 2020.

[130] "dumpcap – Dump network traffic," Wireshark, [Online]. Available: https://www.wireshark.org/docs/man-pages/dumpcap.html. [Accessed 27.08.2021].

[131] "tshark – Dump and analyze network traffic," Wireshark, [Online]. Available: https://www.wireshark.org/docs/man-pages/tshark.html. [Accessed 27.08.2021].

[132] "Perl," Perl.org, [Online]. Available: https://www.perl.org. [Accessed 27.08.2021].

[133] "Umbrella Popularity List," Cisco, 09 2021. [Online]. Available: http://s3-us-west-1.amazonaws.com/umbrella-static/index.html. [Accessed 21.09.2021].

[134] CERT.LV, "Latvija kopā ar sabiedrotajiem veikusi IKT sistēmu draudu meklēšanas operāciju," CERT, 30.11.2022. [Online]. Available: ka ir ārkārtīgi svarīgi nodrošināt tīkla inventarizāciju un redzamību, operētājsistēmu un izmantotās programmatūras savlaicīgus atjauninājumus, sistēmas drošības notikumu apkopošanu un uzraudzību, kā arī reaģēšanu uz incidentiem. [Accessed 07.12.2022].

[135] "SOAR defined," Microsoft, [Online]. Available: https://www.microsoft.com/en-us/security/business/security-101/what-is-soar. [Accessed 23.09.2023].

[136] S. Shea, "SOAR (security orchestration, automation and response)," TechTarget, [Online]. Available: https://www.techtarget.com/searchsecurity/definition/SOAR. [Accessed 26.09.2023].

[137] "CIS Critical Security Controls," CISecurity, [Online]. Available: https://www.cisecurity.org/controls. [Accessed 27.12.2023].

[138] "SOC for Cybersecurity," Aicpa&Cima, [Online]. Available: https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-for-cybersecurity. [Accessed 27.12.2023].

[139] "Cyber Essentials," National Cyber Security Centre, UK, [Online]. Available: https://www.ncsc.gov.uk/cyberessentials/overview. [Accessed 27.12.2023].

[140] S. Cass, "The Top Programming Languages 2023," IEEE, [Online]. Available: https://spectrum.ieee.org/the-top-programming-languages-2023. [Accessed 04.01.2024].

[141] Saeima, "Nacionālās kiberdrošības likums," Saeima, 20.06.2024. [Online]. Available: https://likumi.lv/ta/id/353390-nacionalas-kiberdrosibas-likums. [Accessed 13.01.2025].

[142] K. J. G. J. Minkevičs V., "Managing Information System Security in Higher Education Organizations," in *IEEE Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE)*, Vilnius, Lithuania, 2023.

Vladislavs Minkevičs was born in 1978 in Daugavpils, Latvia. He earned a Bachelor's degree and a Master's degree (2003) in Information Technology from Riga Technical University. He is currently the Head of Information Security at the Central Finance and Contracting Agency. His research interests include cybersecurity, the automation of security operations centres, and the application of artificial intelligence in cybersecurity.