frontiers | Frontiers in Computer Science

TYPE Original Research
PUBLISHED 20 November 2025
DOI 10.3389/fcomp.2025.1692263

OPEN ACCESS

EDITED BY
Dalius Navakauskas,
Vilnius Gediminas Technical University,
Lithuania

REVIEWED BY
Darius Plonis,
Vilnius Gediminas Technical University,
Lithuania
Andrius Katkevicius,
Vilnius Gediminas Technical University,
Lithuania

*CORRESPONDENCE
Vladislavs Minkevics
✉ Vladislavs.Minkevics@rtu.lv

RECEIVED 25 August 2025
ACCEPTED 31 October 2025
PUBLISHED 20 November 2025

CITATION
Minkevics V and Grabis J (2025) A capability-driven automated cybersecurity monitoring and response system. *Front. Comput. Sci.* 7:1692263. doi: 10.3389/fcomp.2025.1692263

A capability-driven automated cybersecurity monitoring and response system

Vladislavs Minkevics* and Jānis Grabis

Faculty of Computer Science, Information Technology and Energy, Riga Technical University, Riga, Latvia

Organizations face a variety of cybersecurity threats, and the implementation of security management solutions is a challenging task. This study proposes to implement such solutions in an incremental manner, starting with key requirements and adding new modules as necessary. A set of key requirements with a focus on cybersecurity threat monitoring and response automation is identified. The capability-driven approach is used to describe these requirements in a structured manner. That enables organizations to identify required security management capabilities in alignment with organizational goals. A cybersecurity monitoring and response system is developed on the basis of the capability model. The system uses machine learning models to identify cybersecurity threats, and appropriate response mechanisms are invoked to deal with the threats. It is shown that the selection of the right adjustments defined in the capability model significantly affects cybersecurity management efficiency. The use of machine learning models also allows the system to adapt to handling new cybersecurity threats. The cybersecurity monitoring and response system is compared with the state-of-the-art commercial systems, and it is shown to achieve a comparable performance while providing a higher level of flexibility.

KEYWORDS

cybersecurity, adaptive cybersecurity, cybersecurity incident management, capability management, machine learning

1 Introduction

Currently, information technology is omnipresent. Both the public and private sectors are dependent on information technologies, and, given the increasing digitalization of the world, this dependence is growing and will likely continue to grow in the future. Information 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 could be used to cause significant damage to public administration information systems and electronic communications networks, neutralize national political, economic, and military decision-making centers, misinform the public, and cause technogenic disasters. This creates an increased 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, one of the most recent initiatives in the European Union being the adoption of the NIS2 Directive (EUR-Lex, 2022). These laws and regulations define minimum requirements for data protection in terms of confidentiality, integrity, and availability, which generally improve cybersecurity. However, cybersecurity incidents are rampant, for example, SolarWinds (Reuters, 2021),

Colonial Pipeline (CNN, 2021), and denial of access attacks against Latvian state institutions (DIENA, 2022). These incidents are often organized by well-funded criminal organizations, various criminal groups, and even countries. These incidents may be prevented should there be appropriate security management in place. 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 an organization. Cyber security 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) (National Institute of Standards and Technology, 2018). The threat detection and proactive threat response phases are crucial for organizations starting to implement security management.

These organizations face several challenges, such as:

- Insufficient source data or timely data (for example, log files that lack the necessary information to identify a cybersecurity incident).
- Different types and structures of source data, which should be normalized and decoded;
- A dynamic network where clients are located in different locations and using different devices at once.
- A data analyst may misinterpret data, which may lead to cybersecurity incidents that are not noticed.
- Insufficient security response scenarios are created, which will require manual response to cybersecurity incidents.

These challenges should be addressed in a holistic manner, and model-driven approaches to security management are used to achieve this goal. The capability-driven development methodology (Grabis et al., 2018) is one of the model-driven approaches, which helps to design security capabilities with respect to the organization's goals. It takes into account context data and invokes adaptive actions to ensure secure operations.

The goal of this study is to develop a Cybersecurity Monitoring and Response System referred to as ISMS using the capability-driven approach and employing machine learning models for adaptive security threats monitoring and response. The system was first introduced in the earlier study (Minkevics et al., 2023). The ISMS system is developed as an extensible and adaptable light-weight cybersecurity management solution, which satisfies the set of requirements with efficiency comparable to large enterprise solutions by major vendors. Its development is based on the capability-driven development approach, which allows organizations to identify their key cybersecurity needs and to design the solution accordingly. The solution can be expanded if new needs arise. It uses big data processing for analysis and identification of security concerns, and data processing pipelines and machine learning models can be adapted according to data availability and security needs.

The rest of the study is organized as follows. Section 2 describes the research methods. The main results on requirements elicitation, capability modeling, and elaboration of adaptive capabilities are presented in Section 3. Section 4 provides discussion and conclusions.

2 Method

In order to address the cybersecurity challenges, both qualitative and quantitative research methods were applied (Figure 1). The qualitative methods are used to identify core requirements for the Cybersecurity Monitoring and Response System and to design the system. The requirements are identified

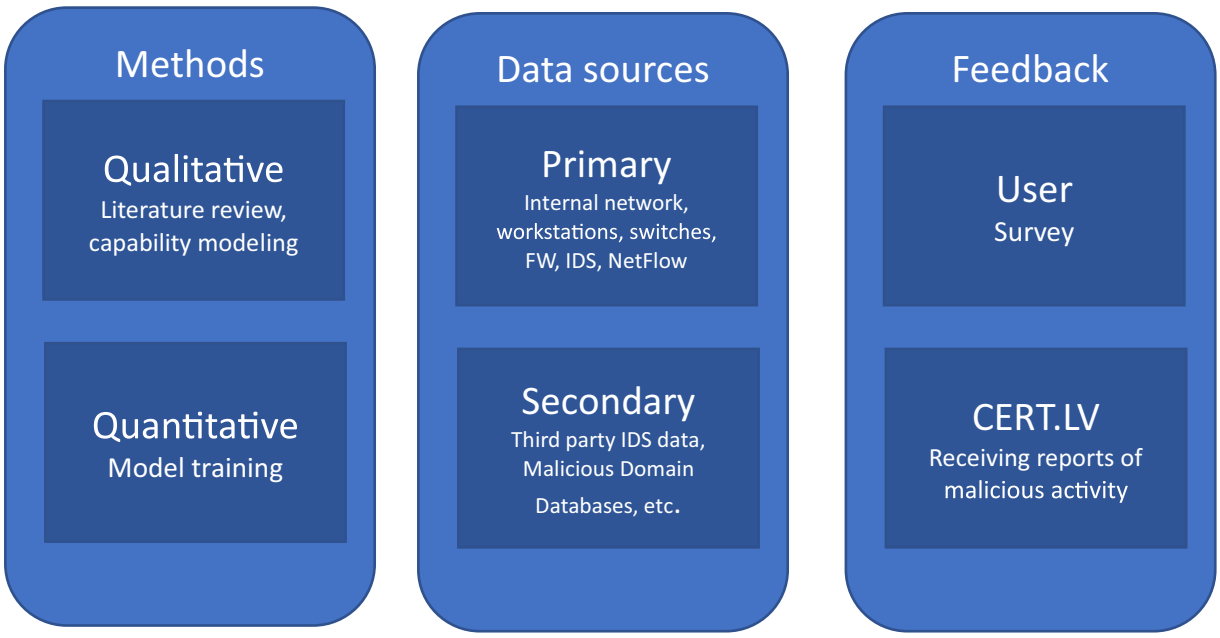

FIGURE 1
Study methodology.

using a literature review, and the system design is performed using the capability-driven approach. Machine learning models are used for threat identification and adaptive response, and the quantitative methods are used for model training. Various data sources are needed to develop the machine learning models. The machine learning models were specifically trained using data from a case company. The primary data sources were data collected from the organization's internal network, user workstations, data provided by network switches, firewall data, intrusion detection system data, NetFlow data, successful/failed authentication, and other audit trail files, and other data sources. The secondary data sources (Alexa, n.d.; Amazon, 2021) 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, as well as an exploration of the domain name request data and manual classification and comparison of suspicious domain name requests against malicious domain databases.

Different feedback mechanisms were used to evaluate the efficiency of the system. The users' survey was conducted to confirm that security threats were correctly identified. Additionally, CERT. LV notifications of malicious activity at the institution were also considered. CERT. LV is the national institution responsible for handling cybersecurity incidents and promoting information technology security in Latvia, and its feedback provides an external confirmation of threat handling at the organization.

The conceptual model underlying the Automated Cybersecurity Monitoring and Response System was developed using the Capability-Driven Development (CDD) (Sandkuhl and Stirna, 2018) approach, as it is suitable for specifying and implementing adaptive solutions. The CDD approach is one of the Enterprise Modeling techniques focusing on enterprise capabilities. While approaches like Archimate allow for the development of comprehensive models of enterprise architecture, the CDD focuses on the incorporation of data-intensive and adaptive features, which are the primary interest in the case of intelligent cybersecurity management (Zdravkovic et al., 2017).

The development of the Automated Cybersecurity Monitoring and Response System proceeds in four steps:

1 Identification of key requirements based on literature analysis;
2 Capability modeling;
3 Solution design and development of core services;
4 Implementation of big data processing-based components for capability delivery.

The literature on big data Automated Cybersecurity Monitoring and Response System is reviewed by analyzing studies published from 2010 to 2024 and referenced in the Scopus database. The following research questions are formulated:

1 What are the typical processes involved in information systems security management? Identify the processes that make up information systems (IS) security management.
2 What data sources are used today to ensure the security of IS? Identify the sources of data used for security analysis and the methods used to process that data.
3 What automated methods and tools are used for IS security management? Identify which automation methods and tools are used today for IS security management.
4 What machine learning techniques are used for IS security management? Identify what machine learning techniques and tools are used to identify unknown threats.
5 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.

The findings from the literature review are used to formulate the key requirements for the cybersecurity management solution. The requirements are further elaborated and formalized using the CDD method. Figure 2 shows the key concepts used in capability modeling, such as goals, capabilities, adjustments, context elements, and measurable properties. The Goal element defines the organization's security goals measured by Key Performance Indicators (KPI). Security capabilities are developed to achieve the goals. The capability delivery is affected by the external context defined by the ContextElement concept. The ContextElement is measured by measurable properties, which are raw data gathered at the organization or externally. The context element provides an interpretation of raw data. The Adjustment element defines adaptive actions invoked in response to changes in the context and aimed at achieving the organization's goals. The capability model is elaborated using these concepts in the design session involving cybersecurity specialists. The initial version of the model was developed following the findings in the literature review, and the model was further refined by the experts.

The Automated Cybersecurity Monitoring and Response System is developed according to the capability model. The data ingestion and pre-processing are developed using Suricata IDS (The Open Information Security Foundation, n.d.) and Apache Kafka (P. S. Foundation, n.d.). In terms of capability-driven development,

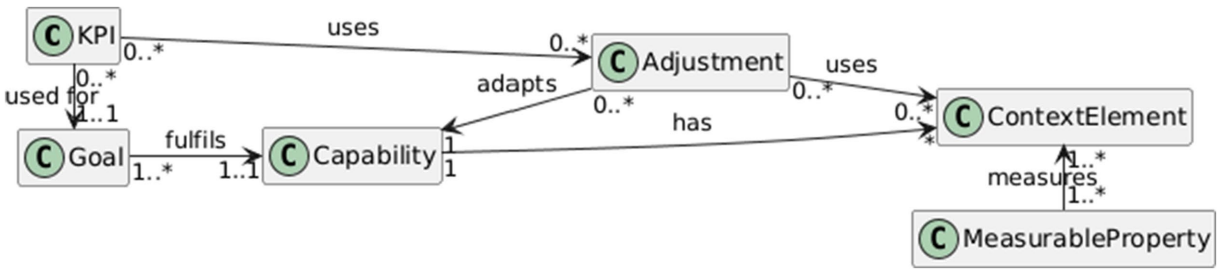

FIGURE 2
Key concepts used in capability modeling.

these systems ensure the retrieval of Measurable Properties. Apache Spark (A. S. Foundation, n.d.) is used to evaluate Context Elements in near real-time (Kampars and Grabis, 2017) using the measurable properties, and Python scripts are used to implement the adjustment. The adjustments include machine learning models used for security threat analysis and automated actions to deal with the security threats. The capability model specifies KPI and context elements used by the adjustments.

3 Results

The automated cybersecurity monitoring and response system was developed following the method outlined in the previous section. The requirements are formulated in Section 3.1. The capability model is specified in Section 3.2. The modules of the system are described in Section 3.3, which also elaborates on machine learning models and response mechanisms used in two of the modules of the system. These sub-sections also include the evaluation of the efficiency of the machine learning models used.

3.1 Requirements

The requirements are identified according to the literature review on methods used for security management. Table 1 lists the analyzed sources of literature. It also indicates the kind of data and technologies used for security management. The findings show that IDS serves as the backbone of the security management solutions. Various data sources, such as audit trails, DNS requests, and Netflow data, are used to monitor the network and to identify threats. The literature sources analyzed rarely consider the integration of security management with big data technologies for real-time data ingestion and stream processing, which might cause scalability issues. Automation scripts are used to supplement IDS functionality and to make security management more efficient. Various machine learning algorithms are used to analyze the aforementioned data streams.

The results of the literature review suggest that data-driven approaches to security management allow for dealing with a variety of threats and adapting to ever-changing circumstances. Accordingly, some of the key data analytical methods for security management are:

(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 behavior, thus identifying, for example, malicious code activity.
(2) System audit trails, which can be used to identify atypical device behavior 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 identify whether firewall rules are working correctly and whether malicious activity has been identified 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 analyzed to identify algorithmically generated domain name requests, which in turn may indicate the presence of a device in the botnet.

The data analytical requirements are combined with the desired characteristics of the extensible light-weight security management solution to formulate the requirements (Table 2). These requirements address core IDS functionality, data analytics, automation, and development aspects. From a development perspective, the proposed solution relies on open-source technologies to achieve cost-efficiency, transparency, and flexibility.

The requirements are also mapped to MITRE ATT&CK Matrix (ATT&CK, 2025). That shows that threats in 11 out of 14 categories are addressed. The main focus areas are Reconnaissance, Discovery, Exfiltration, and Execution in line with the priorities of the monitoring and response systems. The Resource Development, Persistence, and Impact are directly considered.

3.2 Capability model

The capability model is created according to the requirements and discussions at the modeling sessions among the experts. Its purpose is to highlight the required security management capabilities and to design technical solutions for data-driven adaptive security management. The model ensures alignment between organizational requirements and technical solutions supporting these requirements. The capability model focuses on the adaptive behavior of the security management solution, while core parts of the solution are designed following traditional software development techniques.

Figure 3 shows a fragment of the capability model focusing on capabilities and goals. The model defines five key capabilities, starting with Secure network management. This capability is supported by the Automated response to incidents, Protection against DOS and dDOS attacks, Incident prevention, and Secure data processing capabilities. The capabilities allow reaching the goals of monitoring, preventing, and responding to security incidents in a timely manner. For example, the organization has the Goal 3: To ensure availability of systems goal, having the Capability 3: Protection against DOS and dDOS attacks enables achieving this goal. This results in a secure IT environment for employees and builds both internal and external trust in the organization's IT. The goals are measured by their respective KPI (the model fragment shows just exemplary KPI for representation clarity). For example, the Goal 2: To prevent IT security incidents goal is measured by two KPIs, namely, the number of incidents and the incident resolution time. The capability delivery is affected by context, such as Device threat level and User threat level. The context elements provide an actionable interpretation of measurable properties representing raw data measurements (Figure 4).

Figure 4 shows further elaboration of the capability model with a focus on adjustments (i.e., adaptive actions performed during capability delivery). The adjustments are shown for the Secure network management and Automated response incidents capabilities. Devices and users are continuously monitored, and their threat levels are evaluated as an aggregation of measurable properties (i.e., Context

TABLE 1 Properties of security management solutions reported in the literature.

References	Using big data	Use of audit trails	Use of IDS	Use of the honeypot	Network data analysis	Use of DNS	Applying machine learning methods	Using automation scripts	Machine learning algorithms used
Li and Xiao (2010)		x	x		x			x	
Sheng (2019)					x		x		
Ouiazzane (2019)	x	x	x					x	
Shah et al. (2020)			x		x		x		*DTC, K-NN, RFC, SVM*
Sivatha Sindhu et al. (2012)			x				x		*NiB, NNC, DTC*
Sharma et al. (2011)		x	x		x	x			
Rose et al. (2017)		x	x						
Xinyu (2008)					x			x	
Singh et al. (2014)	x				x		x		*RFC, SVM, NiB*
Gupta (2018)			x		x		x		*NNC, Long Short-Term Memory Neural Network*
Raffaele et al. (2020)		x	x						
Muhammet Baykara (2018)			x	x	x				
Hajar Esmaeil As-Suhbani (2019)	x	x					x		*NiB, K-NN, One R, J48*
Plohmann et al. (2016)						x			
Ahluwalia et al. (2017)						x	x		*J48, DTC, RFC*
Truong and Cheng (2016)						x	x		*NiB, J48, RFC, K-NN, SVM*
Selvi and Rodríguez (2019)			x			x	x		*RFC*
Woodbridge et al. (2016)						x	x		*Logistic regression*
Barbosa et al. (2015)						x	x		*Graph*
Mowbray and Hagen (2014)						x			
Peck et al. (2019)						x	x		*NNC, Deep neural network*
Zhong et al. (2019)		x	x				x		*Graph*
Shaukat et al. (2020)			x		x		x		*SVM, DTC, NiB, NNC etc.*
Lewis et al. (2020)						x	x	x	*NiB, RFC, Logistic Regression*
Magalhães and Magalhães (2020)						x	x		*NiB, SVM, DTC, RFC, Logistic Regression, NNC*
Sun et al. (2020)						x	x		*Graph*
Nõmm (2018)					x		x		*K-NN, SVM*
Liu et al. (2019)			x		x	x	x		*OPTICS: Ordering points to identify the clustering structure, GMM (Gaussian mixture models)*

(Continued)

TABLE 1 (Continued)

References	Using big data	Use of audit trails	Use of IDS	Use of the honeypot	Network data analysis	Use of DNS	Applying machine learning methods	Using automation scripts	Machine learning algorithms used
Chkirbene et al. (2020)		x	x		x		x		*RFC, DTC, SVM, "OneClass Support Vector Machine" (OCSVM)*
Elbasiony et al. (2013)			x		x		x		*K-means, RFC*
Mousavi et al. (2020)	x				x	x	x	x	*RFC*
Alguliyev and Imamverdiyev (2014)	x	x	x		x				
Garg (2019)								x	

TABLE 2 Requirements for the automated cybersecurity monitoring and response systems.

No.	Requirement	Mapping with MITRE ATT&CK Matrix
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	Reconnaissance
3	Identify the user and involve them in the security management process	Impact
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	Initial access
6	Use audit trail analysis to identify malicious activity	Execution, exfiltration, collection
7	Use an open-source-based network data analysis mechanism	Discovery, exfiltration
8	Use an open-source-based network metadata analysis mechanism	Discovery, exfiltration
9	Use the honeypot functionality to enable in-depth investigation of malicious code or human activity	Execution, defense evasion, lateral movement
10	Identify theft of user authentication data	Credential access
11	Identify malicious network activity using network metadata and open source-based systems and machine learning	Discovery
12	Detect port scanning and password-guessing activities within the internal network	Reconnaissance
13	Identify and temporarily block external IP addresses that are not involved in any communication—only port scanning	Reconnaissance
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	Command and control
17	Disable devices that pose a threat to the internal network	Lateral movement
18	Display detected incidents and send notifications to the person responsible for security using a graphical interface	–

Element 1: Device threat level is evaluated using six measurable properties as indicated in the model). The detection of malicious activity adjustment uses the context information to identify threats and potential incidents in the volume of network data (machine learning algorithms used in this adjustment are discussed in Section 3.3.1). Minimizing the consequences of an incident adjustment ensures a fast response to severe incidents. The automated response to incidents capability allows organizations to cope with a large number of potential incidents. The User involvement adjustment notifies users of potential incidents (e.g., compromised devices used by the users, identity theft) and provides recommendations on actions to be performed. This adjustment adaptively selects the mode of communication depending on the Level of danger context element (see Section 3.3.2). The mode of communication is selected to optimize the Incident resolution time. The Disconnecting an infected device adjustment is used if the users are not resolving the security incident.

3.3 Solution development

The automated cybersecurity monitoring and response system is implemented to deliver the identified security management capabilities. The solutions architecture has three layers, namely, Data sources, threat detection, and autonomic operations (Figure 5). The threat aggregation and decision-making component orchestrates the threat handling and response activities. The data sources layer contains components for

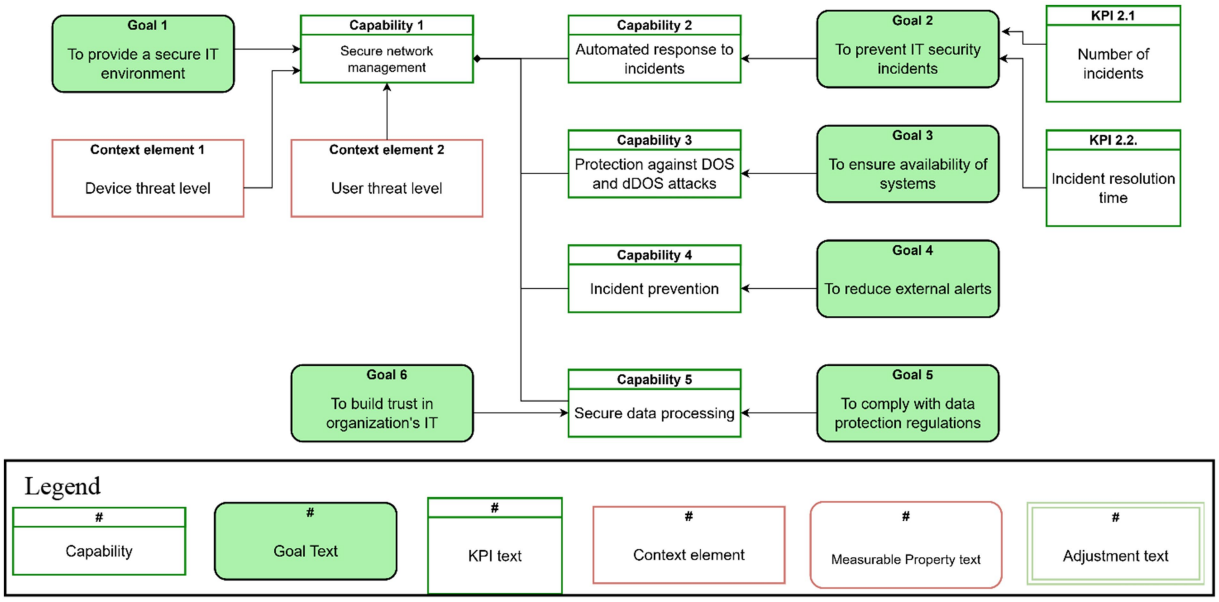

FIGURE 3
A fragment of the capability model focusing on goals.

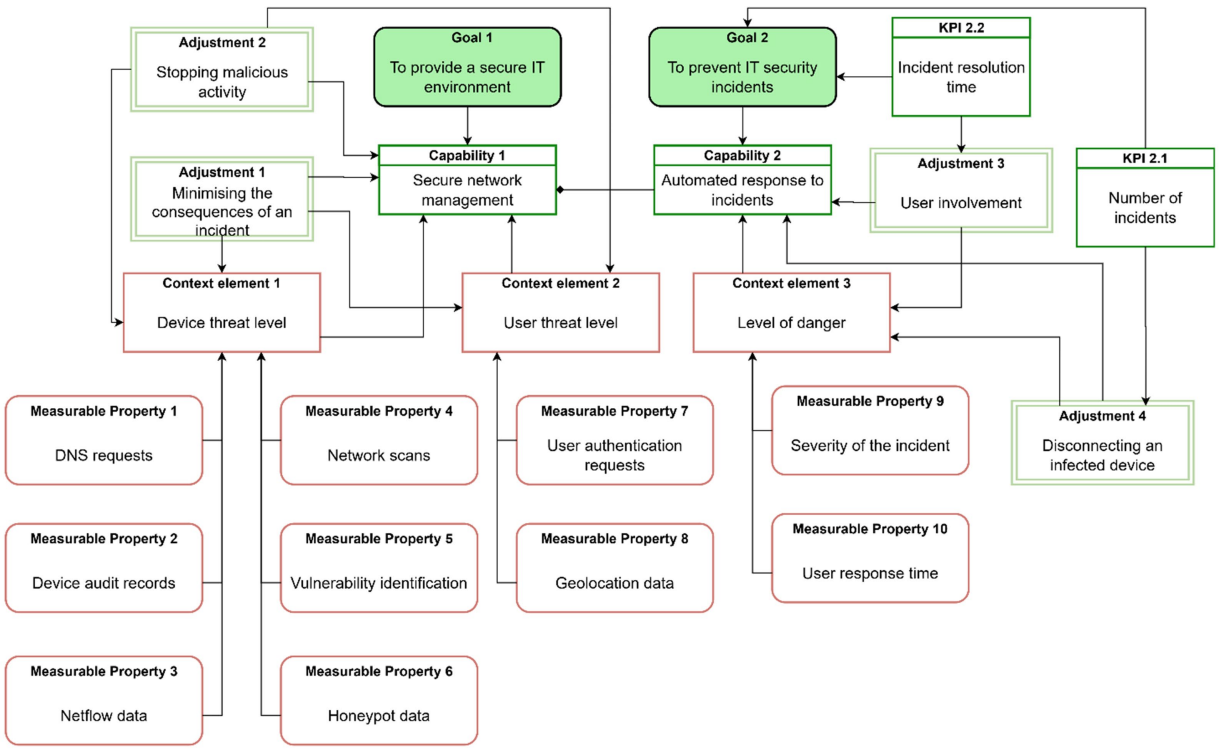

FIGURE 4
A fragment of the capability model focusing on adjustment.

retrieving and pre-processing input data as specified in the requirements. The data includes portal and e-mail system login records, DNS requests, IDS audit trails, firewall audit trails, network switch audit trails, network data, network metadata (NetFlow), DHCP audit trails, server audit trails, and honeypot activity. The data input components correspond to the measurable properties, and data pre-processing leads to the calculation of the context elements in the capability model. For instance, if a user's threat level—as determined by M365 lock data—is elevated, the user is promptly notified via SMS and email, and their immediate involvement is required to address the issue.

The data inputs feed into the second layer, threat detection, which incorporates various analytical modules such as DNS and NFAI machine learning modules, a malicious activity detection module, a vulnerability identification module, a device infection detection module, and a device end-of-life (EOL) detection module. The automatic operations layer facilitates active response mechanisms, including user identification and notification through SMS, e-mail, and an internal portal; system administrator notification via e-mail and the security operations center; and access blocking through wireless access points, switches, and firewalls. The threat detection, together with the automated operations, implements the adjustments defined in the capability model.

The following sub-sections elaborate on the development of components for secure network management and automated response capabilities.

3.3.1 Secure network management

The purpose of secure network management is to prevent malicious activities. Domain generation algorithms (DGA) are used by malware on infected devices to produce potentially malicious requests. Machine learning is used to detect the malicious requests in the DNS machine learning module, which implements Adjustment 2 defined in the capability model - Detecting malicious activity.

A DGA detection model was developed and evaluated, which aimed to find out whether a DNS request generated by the device can be classified as a DGA and thus be considered a malicious request. Experiments were performed on the selection criteria of DGA domains as well as on the construction of feature clusters. A set of features for training DNS classifiers was developed based on the work of Selvi and Rodríguez (2019) study using a set of 10 traits. The DGA module using the RFC machine learning algorithm was trained with 8,856 "bad" and 8,856 "good" domains and was compared with the Palo Alto firewall. 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, the Precision, Accuracy, Recall, and F1-score were measured for each of them using cross-validation. Table 3 shows a comparison of the ML models, showing that RFC gave the best results.

The DGA detection functionality of the system was compared with the up-to-date Palo Alto firewall. The RFC was selected for the DGA model. The evaluation was performed during the period from 1 January 2022 to 31 May 2023. Overall, 13 million DNS requests from different sources have been analyzed by the system during that period, which consisted of 195 thousand unique domain names. The DGA model identified seven additional DNS requests (Table 4) classified as DGA by a third-party source, which were not detected by the Palo

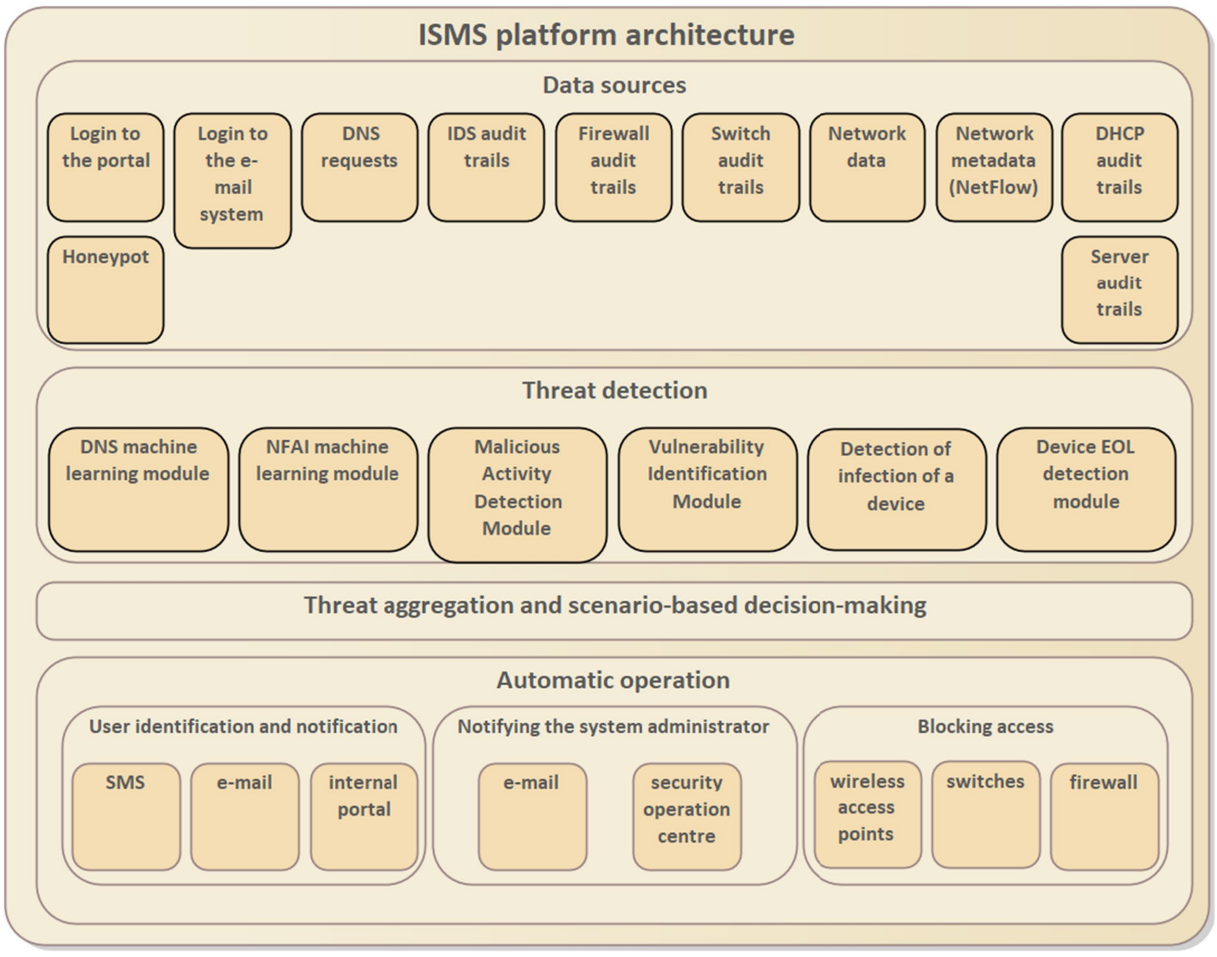

FIGURE 5
Components of the automated cybersecurity monitoring and response system.

Alto firewall (some of them might be false positive identifications). The results indicate that the system achieves results comparable to state-of-the-art proprietary solutions. More information about the model development is presented in Minkevics et al. (2023).

3.3.2 Automated response to incidents

If malicious activities are identified, the system is capable of an automated response to incidents (Capability 1 in Figure 3), and the User involvement adjustment is used for these purposes. The adjustment is implemented in the User identification and notification component. The component supports notification by e-mail and by SMS. The system adaptively chooses the most appropriate notification mode depending on the severity of the threats.

In order to identify the best method of user notification, an experiment was carried out measuring the response time over the same time period as in Section 3.3.1. The user response time was measured by determining the time interval between sending the notification and visiting the university portal. The e-mail message recommended visiting the portal, which provided additional information about the incident, including the IP addresses involved in the incident, as well as other additional information. The user response time to the e-mail recommendations is shown in Figure 6.

On the other hand, alerts that sent information, including via SMS, showed much better results (Figure 6). The majority of users responded to the notification within 5 min. That is also confirmed in the interval plot showing the average response time according to the mode of communication (Figure 7). The logarithmic transformation is applied to the response time to reduce the skewness of the distribution due to several very late responses observed, regardless of the mode of communication. The *t*-test was also performed, yielding t-statistics of 4.13 and a *p*-value of 0.00 for the null hypothesis that there are no differences between the communication modes. That

TABLE 3 Comparison of the ML models.

Classifier	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

TABLE 4 Comparison of the DNS machine learning module with the Palo Alto firewall.

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

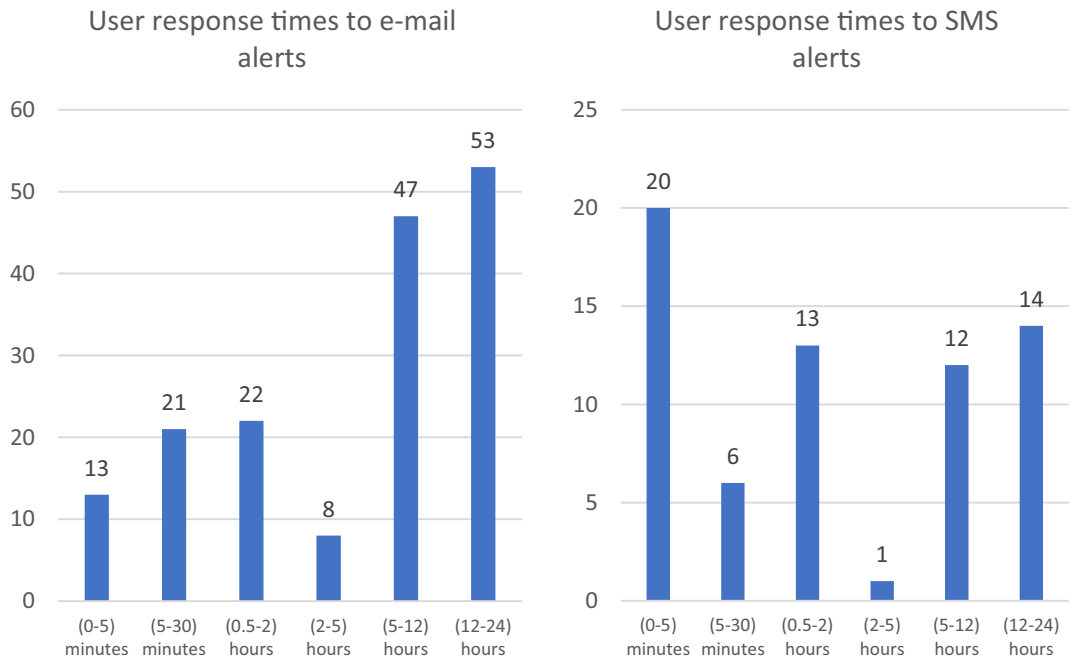

FIGURE 6
The user response to the time to incident notifications sent by e-mail (left) and by SMS (right).

TABLE 5 User feedback.

Action	Number of users
Total feedback provided	123
Feedback that the device was indeed infected	38

shows that the average response times for different means of communication are statistically different. 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.

The users were asked to provide feedback by completing an online questionnaire. A total of 123 unique questionnaires were completed (from 1 January 2021 to 18 May 2023). Some users completed the questionnaire repeatedly, and the duplicate responses were not taken into account. The results (Table 5) show that the use of the ISMS platform has protected 38 users from the threats that could have occurred in the event of an infected device (e.g., leakage of personal data, theft of financial assets). According to the accumulated statistics, more frequent cases of device infections were observed among international students. However, the problem is also that not all international students provide feedback. These results confirm that the proposed ISMS platform is an important component of information systems security and offers the possibility of detecting malware that standard defenses (such as installed antivirus software) do not detect. In total, 104 devices were automatically disconnected from the RTU network during the above-mentioned period, a large number of which were disconnected after the user reported that the device was free of malware. To ensure effective multi-dimensional data analysis to identify security threats, it is necessary to apply big data technologies and machine learning techniques.

4 Discussion

The ISMS system is designed to fulfill the set of key requirements and to deliver core security monitoring and response capabilities specified in the capability model. The evaluation shows that the system provides comparable performance to the state-of-the-art commercial proprietary solutions while providing organizations a possibility for gradually expanding and improving their security management solutions as new threats emerge and new incidents are encountered. This section summarizes the comparison of the ISMS system with selected commercial systems.

4.1 Comparison

The comparative analysis evaluates the ISMS system with two leading commercial solutions [according to Gartner Magic Quadrant leadership benchmarks (IT Security Demand, n.d.)], IBM QRadar and Splunk, based on 13 functional criteria (Table 6). All three tools provide real-time (or near real-time) monitoring, intelligent threat detection, and user activity monitoring. In terms of deployment flexibility, IBM QRadar and Splunk are limited to cloud or specific facility/software installations, whereas the ISMS system supports deployment in the cloud, on standalone machines, or on client systems.

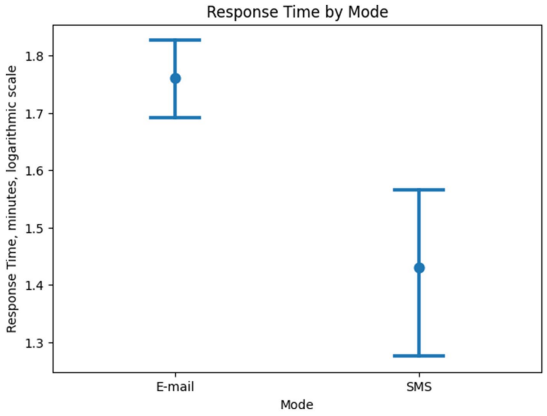

FIGURE 7
The average response time according to the mode of communication.

The ISMS has advantages in its use of artificial intelligence for both botnet identification and aggregated network data analysis, capabilities not available in Splunk and only partially present in IBM QRadar (APT detection). Unlike the private, proprietary nature of IBM QRadar and Splunk, the ISMS is open-source-based. It also supports the seamless addition of organization-specific modules, offers unrestricted scalability, and provides enhanced automated user and administrator involvement during threat events through multiple communication channels (SMS, e-mail, and user portals).

Incident response in IBM QRadar and Splunk involves security personnel, while the ISMS enables automation involving end users and offers automated assistance for incident resolution. Furthermore, the ISMS allows for the rapid programming of additional modules in any programming language, contrasting with the slower, developer-dependent processes in the other platforms.

4.2 Implementation at other organizations

In addition to the Riga Technical University (RTU), ISMS has also been implemented at two Latvian state institutions: the Central Finance and Contracting Agency (CFCA) and the Procurement Monitoring Bureau (PMB). Table 6 summarizes the key observations made on using ISMS at the aforementioned organizations. 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 are separately analyzed in these applications. The log file analysis was integrated in ISMS, reducing fees paid to third-party application developers as well as to proprietary SIEM for handling additional data loads (Table 7).

The value of these features has been confirmed by Chief Information Officers at both organizations. ISMS was also presented to the Latvian information technology security community at the

TABLE 6 Gartner magic quadrant top leader comparison with the ISMs.

No.	Functionality	IBM Q Radar	SPLUNK	ISMS
1	Real-time (or near real-time) monitoring	+	+	+
2	Intelligent threat detection	+	+	+
3	User activity monitoring	+	+	+
4	Installation options	In the cloud or a specific facility	In the cloud or software on client machines	In the cloud, on a standalone machine, or on a client machine
5	Using artificial intelligence to identify botnets	(APT detection)	–	+
6	Platform	Private	Private	Open source-based
7	Adding organization-specific modules	–	– (possibility to configure received audit trails)	+
9	Automated involvement of the user responsible for the resource in the event of a threat	– (informing the person responsible for security)	– (informing the person responsible for security)	+ (SMS/e-mail/user portal)
10	Automated assistance to the resource responsible for resolving a security incident	–	–	+ (SMS/e-mail/user portal)
11	Applying artificial intelligence for the analysis of aggregated network data	–	–	+
12	Incident management	Through the person responsible for IS security	Through the person responsible for IS security	Automated, involving the end user
13	Installation of additional modules	Requires involvement of developer programmers, slow	Requires involvement of developer programmers, slow	Additional modules can be quickly programmed in any programming language

TABLE 7 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
Organization specific modules	Network traffic data analysis module for internal audit to monitor compliance	A module for analyzing 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 instruction while system administrators are involved in specific cases
Incident management	Notification types and notification triggers are tailored to the organization's needs	Notification types and notification triggers are tailored to the organization's needs

CERT. LV seminar "*Be Secure*" in 2023 (CERT.LV, 2023), as well as during the IT security event "*Cyber Commando*" held in Riga, Latvia, in 2024.

4.3 Conclusion

The primary objective of this study was to develop a context-dependent adaptive cybersecurity management system grounded in the capability-driven method and supported by appropriate technical solutions. The proposed system aims to enhance the cybersecurity environment by reducing the frequency of cybersecurity incidents and improving the speed of response to such events.

The literature review shows that analysis of data from various sources is required for comprehensive monitoring and prevention of cybersecurity threats. The capability-driven approach allows formal specification of the usage of these data sources, and machine learning models are efficient in transforming raw data into actionable information for security management. The machine learning model can be updated and expanded if new data or features become available. That increases the flexibility of the cybersecurity management solution. The investigation has been primarily carried out at the RTU, though the implementation of the solution in two other organizations shows that the approach is applicable in different cases.

Various machine learning models are used for detecting security threats in different modules of ISMS. This article discusses

the DGA detection model, while our previous work (Minkevics et al., 2023) discussed the usage of the NetFlow data analysis for the detection of malicious activities. It should be noted that some of the machine learning models can be transferred from one organization to another (e.g., the DGA detection model), while others (e.g., the NetFlow analysis model) should be trained specifically for the organization.

The study argues for using open-source technologies for incremental development of cybersecurity solutions. These technologies, combined with advanced big data processing and machine learning methods, allow the alignment of the cybersecurity management solution with the needs of the organization.

The main limitation of the study is that the comprehensive evaluation of the approach has been performed at a single organization, and machine learning models have been developed using training data from this single organization. However, the platform has been successfully implemented at two other organizations, and performance data are currently being accumulated to evaluate machine learning capabilities.

Data avialbility statement

The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

Author contributions

VM: Writing – original draft, Writing – review & editing. JG: Writing – review & editing, Writing – original draft.

Funding

The author(s) declare that no financial support was received for the research and/or publication of this article.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement

The authors declare that no Gen AI was used in the creation of this manuscript.

Any alternative text (alt text) provided alongside figures in this article has been generated by Frontiers with the support of artificial intelligence and reasonable efforts have been made to ensure accuracy, including review by the authors wherever possible. If you identify any issues, please contact us.

Publisher's note

References

A. S. Foundation. Unified engine for large-scale data analytics. (n.d.) Available online at: https://spark.apache.org/ (Accessed August 12, 2025).

Ahluwalia, A., Traore, I., Ganame, K., and Agarwal, N. (2017). "Detecting broad length algorithmically generated domains" in eds. I. Traore, I. Woungang, A. Awad. Intelligent, Secure, and Dependable Systems in Distributed and Cloud Environments. ISDDC 2017. Lecture Notes in Computer Science, Springer, Cham. Vol. 10618. doi: 10.1007/978-3-319-69155-8_2

Alexa. Alexa Top million domains. (n.d.) Available online at: http://s3.amazonaws.com/alexa-static/top-1m.csv.zip (Accessed August 11, 2021).

Alguliyev, R., and Imamverdiyev, Y. (2014). "Big data: big promises for information security" in 2014 IEEE 8th international conference on application of information and communication technologies (AICT).

Amazon. Alexa top sites (2021). Available online at: https://aws.amazon.com/alexa-top-sites/ (Accessed May 7, 2021).

ATT&CK. The MITRE corporation (2025). Available online at: https://attack.mitre.org/ (Accessed October 10, 2025).

Barbosa, K. R. S., Souto, E., Feitosa, E., and El-Khatib, K. (2015). "Identifying and classifying suspicious network behavior using passive DNS analysis" in 2015 IEEE international conference on computer and information technology; ubiquitous computing and communications; dependable, autonomic and secure computing; pervasive intelligence and computing, 160–167.

CERT.LV. IT security seminar "be secure". (2023). Available online at: https://cert.lv/lv/2023/11/it-drosibas-seminars-esi-dross-decembri (Accessed October 5, 2025).

Chkirbene, Z., Eltanbouly, S., Bashendy, M., Alnaimi, N., and Erbad, A. (2020). "Hybrid machine learning for network anomaly intrusion detection" in 2020 IEEE international conference on informatics, IoT, and enabling technologies, ICIoT 2020, 163–170.

CNN. "Colonial pipeline CEO admits to authorizing $4.4 million ransomware payment," (2021). Available online at: https://edition.cnn.com/2021/05/19/politics/colonial-pipeline-ransom/index.html. (Accessed June10, 2021).

DIENA. (2022). Nedēļas nogalē atvairīti kiberuzbrukumi 70 valsts iestāžu tīmekļa vietnēm. Available online at: https://www.diena.lv/raksts/latvija/zinas/nedelas-nogale-atvairiti-kiberuzbrukumi-70-valsts-iestazu-timekla-vietnem-14280778 (Accessed May 24, 2022).

Elbasiony, R. M., Sallam, E. A., Eltobely, T. E., and Fahmy, M. M. (2013). A hybrid network intrusion detection framework based on random forests and weighted k-means. *Ain Shams Eng. J.* 4, 753–762. doi: 10.1016/j.asej.2013.01.003

EUR-Lex. An official website of the European Union. (2022). Available online at: https://eur-lex.europa.eu/eli/dir/2022/2555 (Accessed September 6, 2023).

Garg, M. D. H.. Securing IoT devices and SecurelyConnecting the dots using REST API and middleware. In: 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU) (2019).

Grabis, J., Zdravkovic, J., and Stirna, J. (2018). "Overview of capability-driven development methodology" in Capability Management in Digital Enterprises. eds. K. Sandkuhl and J. Stirna (Springer). Available online at: https://link.springer.com/chapter/10.1007/978-3-319-90424-5_4#citeas

Gupta, B. B. (2018). Machine learning for computer and cyber security principles, algorithms, and practices. New York: CRC Press Taylor & Francis Group.

Hajar Esmaeil As-Suhbani, S. K. (2019). Classification of firewall logs using supervised machine learning algorithms. *Int. J. Comput. Sci. Eng.* 7, 301–304. doi: 10.26438/ijcse/v7i8.301304

IT Security Demand. 2024 Gartner® magic quadrant™ for SIEM. (n.d.) Available online at: https://www.itsecuritydemand.com/whitepaper/security/2024-gartner-magic-quadrant-for-siem/ (Accessed August 1, 2025).

Kampars, J., and Grabis, J. (2017). "Near real-time big-data processing for data driven applications" in International conference on big data innovations and applications (innovate-data) (Prague).

Lewis, J. L., Tambaliuc, G. F., Narman, H. S., and Yoo, W. S. (2020). "IP reputation analysis of public databases and machine learning techniques" in International conference on computing, networking and communications, ICNC 2020. (Big Island, HI, US: IEEE).

Li, L., and Xiao, D. (2010). "Research on the network security management based on data mining" in 2010 3rd international conference on advanced computer theory and engineering (ICACTE) (Chengdu).

Liu, J., Tian, Z., Zheng, R., and Liu, L. (2019). A distance-based method for building an encrypted malware traffic identification framework. *IEEE Access* 7, 100014–100028. doi: 10.1109/ACCESS.2019.2930717

Magalhães, F., and Magalhães, J. P. (2020). "Adopting machine learning to support the detection of malicious domain names" in 7th international conference on internet of things: Systems, management and security, IOTSMS 2020.

Minkevics, V., Grabis, J., and Kampars, J. (2023). "Managing information system security in higher education organizations" in Managing information system security in higher education organizations, IEEE workshop on advances in information, electronic and electrical engineering (AIEEE) (Vilnius).

Mousavi, S. H., Khansari, M., and Rahmani, R. (2020). A fully scalable big data framework for botnet detection based on network traffic analysis. *Inf. Sci.* 512, 629–640.

Mowbray, M., and Hagen, J. (2014). "Finding domain-generation algorithms by looking at length distribution" in 2014 IEEE international symposium on software reliability engineering workshops.

Muhammet Baykara, R. D. (2018). A novel honeypot based security approach for real-time intrusion detection and prevention systems. *J. Inf. Secur. Appl.* 41, 103–116.

National Institute of Standards and Technology, "Framework for improving critical infrastructure cybersecurity. (2018). Available online at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (Accessed June 8, 2020).

Nõmm, H. B. S. (2018). "Unsupervised anomaly based botnet detection in IoT networks" in 2018 17th IEEE international conference on machine learning and applications (ICMLA).

Ouiazzane, M. A. F. B. S. (2019). "A multi-agent model for network intrusion detection" in 2019 1st international conference on smart systems and data science (ICSSD).

P. S. Foundation. Apache Kafka. (n.d.). Available online at: https://kafka.apache.org/ (Accessed August 12, 2025).

Peck, J., Nie, C., Sivaguru, R., Grumer, C., Olumofin, F., Yu, B., et al. (2019). Charbot: a simple and effective method for evading DGA classifiers. *IEEE Access* 7, 91759–91771. doi: 10.1109/ACCESS.2019.2927075

Plohmann, F. F. D., Yakdan, U. O. B. K., Klatt, D. M., Bader, J., and Gerhards-Padilla, F. F. E. (2016). "A comprehensive measurement study of domain generating malware" in 25th USENIX security symposium (Austin, TX).

Raffaele, M. C., Corte, D., and Pecchia, A. (2020). Contextual filtering and prioritization of computer application logs for security situational awareness. *Futur. Gener. Comput. Syst.* 111, 668–680.

Reuters. SolarWinds hack was 'largest and most sophisticated attack' ever. (2021). Available online at: https://www.reuters.com/article/us-cyber-solarwinds-microsoft-idUSKBN2AF03R (Accessed April 26, 2021).

Rose, I., Felts, N., George, A., Miller, E., and Planck, M. (2017). "Something is better than everything: a distributed approach to audit log anomaly detection" in IEEE cybersecurity development (SecDev).

Sandkuhl, K., and Stirna, J. (2018). Capability Management in Digital Enterprises: Springer International Publishing, 396. Available online at: https://link.springer.com/book/10.1007/978-3-319-90424-5#accessibility-information

Selvi, E.-O. J., and Rodríguez, R. J. (2019). Detection of algorithmically generated malicious domain names using masked N-grams. *Elsevier* 124, 156–163.

Shah, A., Clachar, S., Minimair, M., and Cook, D. (2020). "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.

Sharma, A., Kalbarczyk, Z., Barlow, J., and Iyer, R. (2011). "Analysis of security data from a large computing organization" in IEEE/IFIP 41st international conference on dependable systems & networks (DSN), 506–517.

Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., and Xu, M. (2020). A survey on machine learning techniques for cyber security in the last decade. *IEEE Access* 8, 222310–222354. doi: 10.1109/ACCESS.2020.3041951

Sheng, M. (2019). Machine learning for computer and cyber security principles, algorithms, and practices. New York: CRC Press Taylor & Francis Group.

Singh, K., Guntuku, S. C., Thakur, A., and Hota, C. (2014). Big data analytics framework for peer-to-peer botnet detection using random forests. *Inf. Sci.* 278, 488–497. doi: 10.1016/j.ins.2014.03.066

Sivatha Sindhu, S. S., Geetha, S., and Kannan, A. (2012). Decision tree based light weight intrusion detection using a wrapper approach. *Expert Syst. Appl.* 39, 129–141. doi: 10.1016/j.eswa.2011.06.013

Sun, X., Yang, J., Wang, Z., and Liu, H. (2020). "HGDom: heterogeneous graph convolutional networks for malicious domain detection" in NOMS 2020–2020 IEEE/IFIP network operations and management symposium.

The Open Information Security Foundation. Suricata. (n.d.). Available online at: https://suricata.io/ (Accessed August 12, 2025).

Truong, D.-T., and Cheng, G. (2016). Detecting domain-flux botnet based on DNS traffic features in managed network. *Secur. Commun. Netw.* 9, 2338–2347. doi: 10.1002/sec.1495

Woodbridge, J., Anderson, H. S., Ahuja, A., and Grant, D. (2016). Predicting domain generation algorithms with long short-term memory networks. Arlington, VA: Endgame, Inc., 13.

Xinyu, W. Z. A. W. (2008). "NetFlow based intrusion detection system" in 2008 international conference on MultiMedia and information technology.

Zdravkovic, J., Stirna, J., and Grabis, J. (2017). A comparative analysis of using the capability notion for congruent business and information systems engineering. *Complex Syst. Inform. Model. Q.*, 1–10.

Zhong, C., Yen, J., Liu, P., and Erbacher, R. F. (2019). Learning from experts' experience: toward automated cyber security data triage. *IEEE Syst. J.* 13, 603–614. doi: 10.1109/JSYST.2018.2828832