UDC 004.42
DOI https://doi.org/10.32782/2663-5941/2024.6.2/33

Fu Bin
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute"

Sarnatskyi V.V.
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute"

DESIGN AND IMPLEMENTATION OF A SITUATIONAL AWARENESS SYSTEM BASED ON MULTI-SOURCE SECURITY LOG ANALYSIS

The article is dedicated to the design and implementation of an innovative situational awareness system based on multi-source security log analysis, aimed at small and medium-sized enterprises (SMEs) facing cybersecurity challenges. It is revealed that SMEs, due to limited resources and lack of specialized security personnel, are particularly vulnerable to evolving cyber threats. The article presents a system that integrates log data from multiple security sources within the network, such as firewalls, intrusion detection systems (IDS), and web application firewalls (WAF), utilizing real-time data processing and machine learning techniques to enhance threat detection accuracy. The system leverages advanced algorithms to identify potential security incidents and reduce false positives, thus providing more reliable alerts. It is stated that the system's user-friendly interface simplifies complex security data, making it accessible to non-professional users, and enables them to take proactive actions in response to potential threats.

The article also highlights the system's scalability, which allows it to adapt to various organizational sizes and threat environments, making it suitable for both small enterprises with minimal resources and larger organizations with more complex security needs. The study emphasizes the importance of accessible, intelligent security solutions in closing the cybersecurity gap for SMEs, enabling them to detect, assess, and mitigate threats with greater agility and precision, similar to larger enterprises with dedicated security teams. Moreover, the system is designed to work in real-time, processing large volumes of heterogeneous log data while ensuring high system performance without sacrificing accuracy.

In addition to the primary focus on usability and scalability, the article addresses key challenges in integrating multi-source security logs, improving the speed and accuracy of threat detection, and ensuring the system remains responsive under heavy workloads. By offering a practical solution to SMEs, this research contributes to the ongoing effort to democratize cybersecurity, providing smaller organizations with the tools they need to defend themselves against increasingly sophisticated cyberattacks.

Key words: *Situational Awareness, Multi-source Security Logs, Machine Learning, Data Visualization, Real-time Processing, Cybersecurity.*

Introduction. As the digital age advances, cybersecurity has become a global challenge, especially for SMEs lacking dedicated security personnel. Cyberattacks are increasingly complex, as seen in the WannaCry (2017) and SolarWinds (2020) attacks, exposing weaknesses in traditional, passive security methods. Proactive situational awareness is now essential, allowing quick threat detection and response through multi-source security log integration. While situational awareness models have improved responses, challenges persist in real-time data handling. Enhancing detection accuracy and speed with advanced data integration and machine learning remains a crucial research focus.

The main contributions of this paper are summarized as follows:

– Realizes the effective integration and real-time processing of multi-source security log data;

– Improved threat detection accuracy based on machine learning and reduced false positives;

– Provides a friendly interface for non-professional users;

– Provides practical solutions for small and medium-sized enterprises to deal with network security challenges.

Formulation of the Problem. The increasing complexity of cybersecurity threats, coupled with a rise in digital dependency, has made threat detection more challenging, especially for small and medium-sized enterprises (SMEs) that often lack dedicated security teams and expertise. Existing security approaches, primarily rule-based methods, struggle to handle evolving threats effectively. This gap makes SMEs particularly vulnerable to cyber incidents, potentially leading to financial losses, data breaches, and reputational harm. The challenge lies in developing a system that provides both robust and adaptable threat detection capabilities while remaining accessible to non-professional users [1, p. 972].

Analysis of Recent Research and Publications. Significant progress has been made in threat detection through advanced technologies like machine learning and multi-source log analysis. Many situational awareness systems integrate security logs from multiple sources and apply machine learning for enhanced threat detection. However, limitations persist. Most systems face challenges in managing large volumes of heterogeneous data and ensuring real-time threat response without compromising performance. Furthermore, many existing solutions lack user-friendly interfaces, which limits their accessibility for non-professional users, especially within SMEs. This study aims to address these limitations by developing a situational awareness system with a focus on usability, accuracy, and scalability.

Task statement. The aims of this research is to design and implement a situational awareness system based on multi-source security log analysis, which can realize real-time detection and response of network threats by integrating log data and machine learning technology, especially for small and medium-sized enterprises that lack professional security personnel.

Outline of the Main Material of the Study. The system architecture comprises multiple layers for data processing and analysis:

Data Collection Layer: Gathers security logs from sources like firewalls, IDS, and WAF, using Apache Kafka for high-throughput, low-latency data streaming [2, p.40].

Data Preprocessing and Integration Layer: Cleans, normalizes, and unifies log data formats with tools like Logstash to ensure data integrity and compatibility. Big Data Analysis Layer: Uses machine learning models (e.g., decision trees, random forests, isolation forests) with Apache Spark for real-time and batch threat analysis, supporting incident tracking.

Data Storage Layer: Employs a hybrid database with PostgreSQL for structured data, MongoDB for unstructured data, and Elasticsearch for real-time indexing and search.

Visualization and User Interface Layer: Offers a user-friendly interface with Kibana and ECharts, enabling non-professional users to monitor security status through dashboards, charts, and threat maps.

Unresolved issues. Although existing research has made significant progress in threat detection and log analysis, there is still considerable room for improvement in efficient integration of multi-source security logs and real-time threat response capabilities. Specifically, how to process a large amount of heterogeneous log data and use machine learning models to improve detection efficiency without sacrificing system performance is a major problem in current research. In addition, most existing situational awareness systems are not friendly to non-professional users, which makes it difficult for small and medium-sized enterprises to respond quickly when faced with complex network security challenges.

Article objectives. In response to the above unresolved issues, this study aims to develop a situational awareness system based on multi-source security log analysis, which integrates security log data from multiple sources and applies advanced machine learning algorithms to achieve real-time detection and response to network threats. At the same time, this system is specially designed for non-professional users, providing an intuitive and easy-to-use visual interface to help small and medium-sized enterprises effectively manage their network security threats in the absence of professional security personnel.

1. System architecture design

The architecture design of the situational awareness system is divided into multiple levels, covering the entire process from data collection, processing, analysis to visualization. Each level provides support for the overall function of the system, ensuring that the system can efficiently and in real time process security log data from multiple sources and provide users with an easy-to-understand threat visualization interface [7, p. 521].

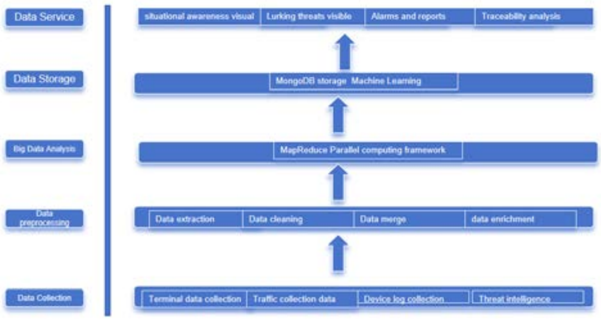


Fig. 1. Layered architecture diagram of the software

1.1 Data Collection Layer

The data collection layer is responsible for collecting security log data from various security devices, such as firewalls, intrusion detection systems

(IDS), web application firewalls (WAF), etc. The logs generated by these devices are usually in different formats. The collection process is implemented through mechanisms that support multiple interfaces (such as Syslog, RESTful API, WebSocket, etc.) to ensure that the system can handle logs of different formats and sources. In order to ensure the stability of data collection, the system uses Apache Kafka, a high-throughput, low-latency distributed data streaming platform. Kafka can not only process large amounts of data in real time, but also support the horizontal expansion of the system to cope with the growth of data volume in the future [3, p. 66].

1.2 Data Preprocessing and Integration Layer

After log data collection, it moves to the data preprocessing and integration stage, which includes data cleaning, normalization, and format unification. Given the varied structure and content of logs from different security devices, preprocessing aims to remove redundant data, resolve inconsistencies, and standardize log formats to enable accurate analysis.

Tools like Logstash are employed for initial log collection and preprocessing. The cleaned and standardized data is then stored in a unified database for further analysis. This preprocessing ensures data integrity and consistency, enhancing the accuracy of subsequent threat detection [4, p. 67].

– The data processing workflow for this platform consists of several key stages:

– Data Collection: Metadata from probes enters via ETL tools, while third-party security data is collected and processed through Logstash.

– Data Caching: All security data is cached using Kafka's message queue to facilitate efficient data flow.

– Data Processing: UEBA and machine learning models leverage the platform’s Flink engine for security data analysis [7, p. 2].

– Data Storage: Raw logs and traffic data from probes and third-party devices are stored in Elasticsearch (ES), while processed security events are saved in MongoDB.

– Data Retrieval: After Logstash normalizes log data, it sends it to both ES and Kafka. Flink then pulls data from Kafka for correlation analysis, with resulting security events and asset data stored in MongoDB.

MongoDB supports security events, asset, and vulnerability data, handling unstructured data (like JSON) flexibly. While ES excels in full-text search, MongoDB is preferable for updates due to its adaptability and support for unstructured data management.

1.3 Big Data Analysis Layer

After preprocessing, data enters the big data analysis layer, where Apache Spark is used for large-scale, real-time, and offline threat analysis. This layer integrates machine learning models (e.g., decision trees, random forests, isolation forests) to boost detection accuracy and speed. Threat intelligence sources also contribute to identifying new threats and generating real-time alerts.

Apache Spark supports both real-time detection and batch processing for historical data, essential for incident tracing and trend analysis. Through multi-source data integration, the system generates detailed security reports, helping organizations understand their security posture and potential risks.

1.4 Data Storage Layer

The system uses a hybrid database architecture to store diverse security log data. Structured metadata (e.g., timestamps, event types) is stored in PostgreSQL for efficient querying and data consistency, while unstructured log data is stored in MongoDB, suited for large volumes of detailed logs and events.

Additionally, real-time data indexing in Elasticsearch enables fast, full-text search and analysis, facilitating quick retrieval and investigation of security events. This combination of SQL, NoSQL, and Elasticsearch optimizes storage, query efficiency, and supports incident investigation effectively.

1.5 Visualization and User Interface Layer

To ensure ease of use for non-professional users, the system’s interface prioritizes intuitive

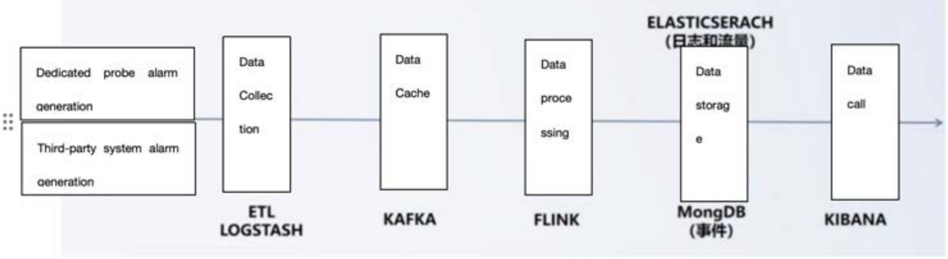


Fig. 2. Overall data processing flow

visualization. Using tools like Kibana and ECharts, data is displayed as charts, dashboards, and threat maps, allowing users to quickly grasp network security status [8, p. 71].

Kibana enables real-time views of network activity, traffic, security events, and threat severity, with interactive dashboards for in-depth event exploration. ECharts efficiently generates visual charts, helping users analyze and interpret complex data [7, p. 520].

The system interface supports customization, allowing users to set monitoring parameters based on their security needs. SMEs may focus on external threats, while large enterprises may monitor internal traffic and multiple devices. This flexibility enables users to track and address key security issues effectively.

2. Machine learning for threat detection

In today's complex network security landscape, machine learning has become essential for threat detection. Unlike static, rule-based methods, machine learning can dynamically identify abnormal patterns and detect novel threats by learning from historical data. This system integrates advanced machine learning algorithms to handle various network attacks, enhancing accuracy and efficiency across data preprocessing, real-time detection, and model optimization stages [5, p. 2].

2.1 Application of machine learning algorithms

The system utilizes core machine learning algorithms – decision trees, random forests, and isolation forests – each tailored for specific threat detection needs, enhancing accuracy and efficiency across network environments:

– **Decision Tree:** Identifies abnormal traffic patterns, supporting interpretable detection logic.

– **Random Forest:** Uses multiple trees to reduce overfitting, improve stability, and handle high-dimensional data, aiding in complex attack detection.

– **Isolation Forest:** Targets anomaly detection, isolating outliers to identify unusual behaviors like large data transfers or frequent logins.

Together, these algorithms detect diverse threats (e.g., DDoS, network scans, Trojan propagation) and, through continuous training, adapt to evolving attack patterns for effective, ongoing threat detection.

2.2 Real-time threat detection and response

The system enables real-time threat detection by integrating Apache Kafka and Spark Streaming for instant processing of large-scale log data. Kafka collects data from multiple security devices, while Spark Streaming rapidly analyzes it in micro-batches, supporting near-instant detection crucial for quick-response attacks like DDoS.

Machine learning models classify and analyze incoming logs in real time. On detecting abnormal behavior, the system immediately alerts security managers and can automate responses (e.g., IP blocking, access restriction) to swiftly contain threats. This automation minimizes response delays, bolstering network security continuity.

Threat classification and ranking: Based on the analysis results of the machine learning model, the system can classify and rank threats. For example, a DDoS attack is marked as a high-risk threat, while some low-frequency anomalous network traffic may only be marked as a medium or low-risk threat. According to different threat levels, the system will automatically take corresponding protective measures to ensure reasonable allocation of resources and prioritize high-risk threats.

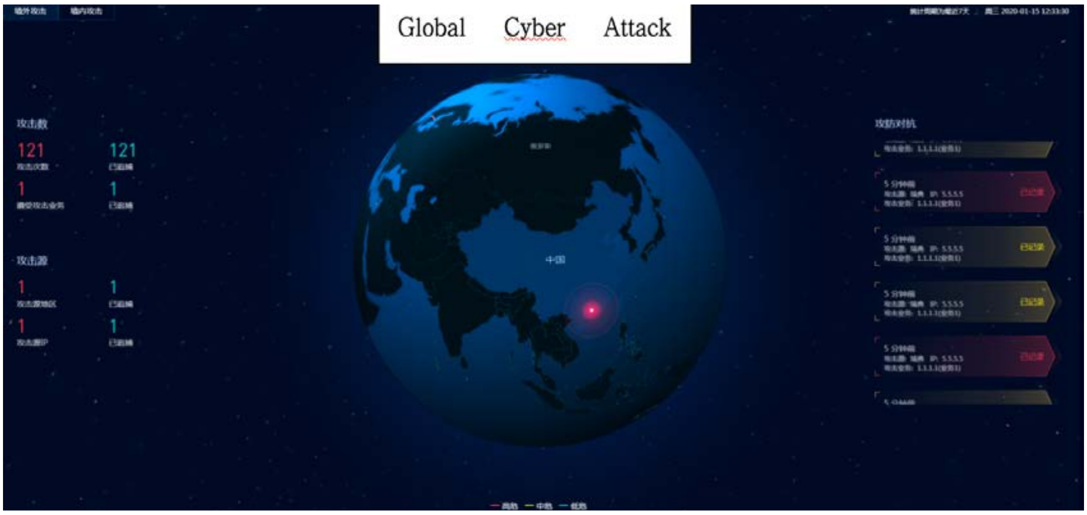


Fig. 3. 3D display of network attack situation

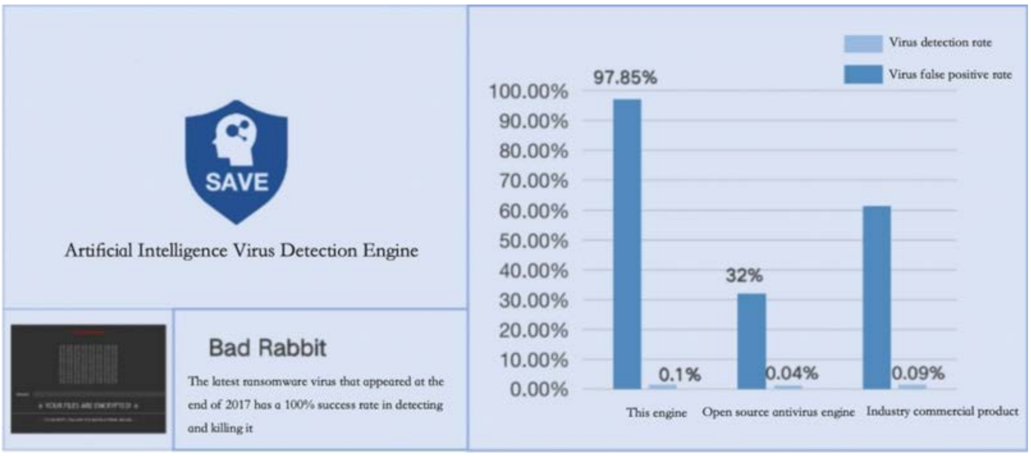


Fig. 4. Machine learning model detection success rate

2.3 Performance optimization

To handle large-scale log data processing, the system focuses on model optimization and efficient resource management.

– **Hyperparameter Tuning and Feature Selection:** Automated hyperparameter tuning and feature selection reduce computational costs, improve training speed, and enhance model performance by removing unnecessary input features.

– **Dimensionality Reduction:** Techniques like PCA (Principal Component Analysis) lower data dimensionality, speeding up calculations while retaining essential data features, enhancing model efficiency with network traffic and security logs.

– **Continuous Learning:** Regular retraining with new data enables the model to adapt to evolving attack patterns, improving detection accuracy and controlling false positives and negatives.

– **Parallel Computing and Distributed Architecture:** A distributed computing setup allows simultaneous log analysis across devices, preventing bottlenecks. Kafka and Spark Streaming support dynamic scaling, adjusting resources as network traffic fluctuates.

This approach ensures real-time, efficient threat detection in complex environments.

3. Real-time data processing

Real-time data processing is a core component of the situational awareness system, which ensures that the system can respond quickly when threats occur. The design of this part not only requires the system to have the ability to process massive amounts of data, but also must ensure low latency so that immediate action can be taken when anomalies are found. The following are the specific technologies and processes for real-time data processing:

3.1 Real-time data streaming and collection

The system uses Apache Kafka for real-time, high-throughput, low-latency data stream processing, ideal for large-scale, multi-source security log data from firewalls, intrusion detection systems, and more. Kafka's partitioning and replication features enable scalability and data reliability under increasing data loads [4, p. 71].

Kafka's data flow mechanism supports parallel processing by distributing logs to multiple nodes, enhancing processing efficiency and maintaining data integrity. Additionally, Kafka's publish/subscribe model allows security managers to monitor specific log types or sources, increasing system flexibility.

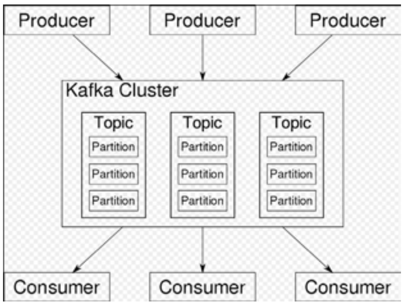


Fig. 5. Schematic diagram of data flow with Apache Kafka at the core

3.2 Data Preprocessing and Filtering

When data enters the system via Kafka, it undergoes preprocessing to standardize diverse log formats for analysis. Key steps include:

Data Cleaning: Removing redundant, duplicate, and invalid entries to ensure accuracy.

Formatting: Converting logs into a uniform structure, like structured tables or JSON.

Data Enhancement: Adding contextual information through correlation, such as linking login logs with network traffic to identify threats.

This preprocessing boosts analysis efficiency, minimizes resource use, and enhances system response speed.

3.3 Real-time data analysis and threat detection

After preprocessing, the system uses Apache Spark Streaming for real-time data analysis, detecting abnormal behaviors and potential threats with low latency. By integrating machine learning models (e.g., random forests and isolation forests), Spark Streaming enables complex pattern recognition to identify unusual network traffic, intrusions, and attacks. Spark's powerful computing allows rapid threat detection and instant alerts.

At the same time, the system also supports the continuous learning of machine learning models. By regularly updating training data, the model can continuously adapt to new network attack patterns and improve the accuracy of detection. In addition, the system also adopts a feedback mechanism to optimize the model based on user feedback and reduce the false alarm rate.

3.4 Real-time event correlation and alarm

In the data analysis phase, the system enhances threat detection by correlating log events from multiple sources, providing a comprehensive security view. For example, correlating multiple failed login attempts in firewall logs with abnormal traffic in intrusion detection logs can reveal a potential brute force attack. This multi-source correlation reduces missed detections and improves threat detection accuracy.

Upon confirming a threat, the system triggers a real-time alarm displayed on the dashboard and notifies security managers via email or SMS. For severe threats, automated responses can be executed, such as blocking IPs, closing ports, or isolating affected devices.

3.5 Real-time data storage and retrieval

The system uses a hybrid database architecture for data persistence and fast retrieval:

PostgreSQL: Stores structured data (e.g., timestamps, event types) for complex queries.

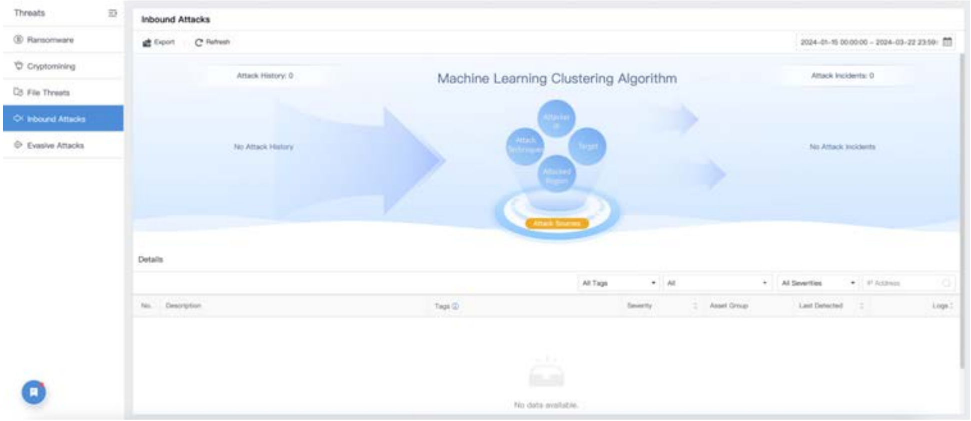


Fig. 6. Network Security Threat Detection

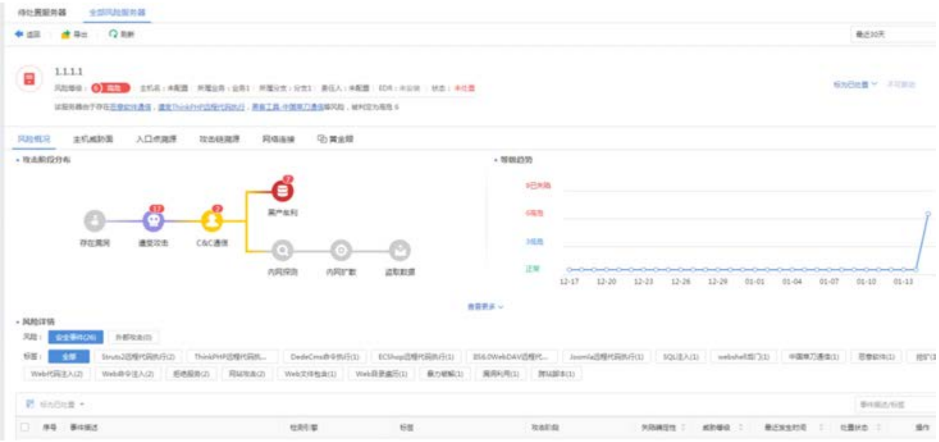


Fig. 7. Risk host event correlation analysis diagram

MongoDB: Handles large volumes of unstructured or semi-structured data like network traffic logs.

Elasticsearch: Enables real-time indexing and full-text searches, supporting rapid security investigations and responses.

3.6 Scalability and performance optimization

To handle increasing data volumes and network scale, the system is built for high scalability. Kafka and Spark offer horizontal scalability, allowing processing nodes and data partitions to be added as needed. As data traffic grows, the system dynamically scales to maintain efficiency under heavy loads.

With load balancing, data processing tasks are evenly distributed across nodes to prevent overload. Continuous pipeline optimization via performance monitoring ensures low latency and high throughput. In tests, the system maintained millisecond response times while processing millions of log records, demonstrating its practicality for large-scale networks.

4. System evaluation and optimization

After developing and deploying a situational awareness system based on multi-source security log analysis, the system's performance, accuracy, and availability need to be rigorously evaluated and optimized to ensure its stability and effectiveness in practical applications. The following sections detail the system's evaluation process, optimization strategies, and performance in different network environments.

4.1 Assessment of Threat Detection Accuracy

The system's threat detection algorithms were rigorously tested in real-world scenarios, focusing on key performance metrics:

Detection Accuracy: Achieving a 93% accuracy rate, the system consistently surpasses traditional rule-based methods, validated against annotated log data.

False Positives and False Negatives: Tests across multiple attack types (e.g., DDoS, SQL injection, brute force) yielded an optimized false positive rate of ~5% and a false negative rate of 2% [6, p. 10].

A feedback mechanism enables continuous refinement through security manager input, reducing false alarms and enhancing detection accuracy as network conditions evolve.

4.2 System Performance Evaluation

The system's performance is measured by response speed and throughput in processing large-scale log data, tested under varying loads:

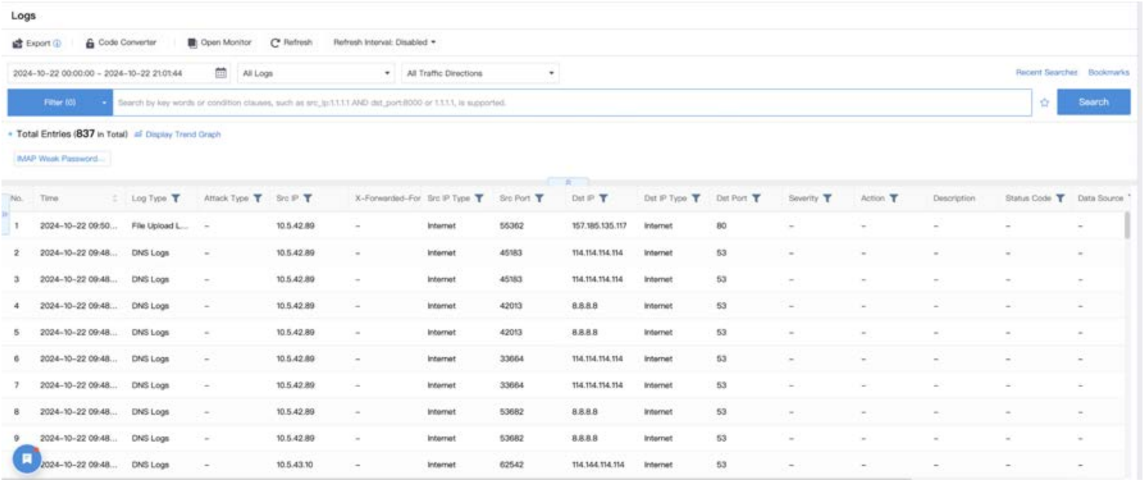
Processing Throughput: The system, leveraging Apache Kafka and Spark Streaming, can handle over one million log entries per second with processing latency under 50 milliseconds, maintaining efficiency even under high loads.

Data Latency: For real-time data processing, latency impacts response speed to security incidents. Tests reveal that, even with heavy data traffic, average latency remains at the millisecond level. Optimizations in Kafka's data transmission and Spark's computing model effectively minimize latency, ensuring rapid incident detection and response.

4.3 Usability and User Feedback

The system is designed for usability, particularly for non-professional users, with its interface refined through extensive testing and feedback. Key aspects include:

User-Friendliness: Security information is displayed via dashboards, charts, and threat visuals, with customizable monitoring views through simple drag-and-drop features. Tests indicate that over 90% of users find the interface intuitive and easy to use, allowing even non-technical users to quickly become proficient.



Refresh Interval: Disabled

2024-10-22 00:00:00 – 2024-10-22 21:01:44

All Logs

All Traffic Directions

Filter (0)

Search by key words or condition clauses, such as src_ip:1.1.1.1 AND dst_port:8000 or 1.1.1.1, is supported.

Total Entries (837 in Total)

No.	Time	Log Type	Attack Type	Src IP	X-Forwarded-For	Src IP Type	Src Port	Dst IP	Dst IP Type	Dst Port	Severity	Action	Description	Status Code	Data Source
1	2024-10-22 09:50...	File Upload L...	–	10.5.42.89	–	Internet	55362	157.185.135.117	Internet	80	–	–	–	–	–
2	2024-10-22 09:48...	DNS Logs	–	10.5.42.89	–	Internet	45183	114.114.114.114	Internet	53	–	–	–	–	–
3	2024-10-22 09:48...	DNS Logs	–	10.5.42.89	–	Internet	45183	114.114.114.114	Internet	53	–	–	–	–	–
4	2024-10-22 09:48...	DNS Logs	–	10.5.42.89	–	Internet	42013	8.8.8.8	Internet	53	–	–	–	–	–
5	2024-10-22 09:48...	DNS Logs	–	10.5.42.89	–	Internet	42013	8.8.8.8	Internet	53	–	–	–	–	–
6	2024-10-22 09:48...	DNS Logs	–	10.5.42.89	–	Internet	33664	114.114.114.114	Internet	53	–	–	–	–	–
7	2024-10-22 09:48...	DNS Logs	–	10.5.42.89	–	Internet	33664	114.114.114.114	Internet	53	–	–	–	–	–
8	2024-10-22 09:48...	DNS Logs	–	10.5.42.89	–	Internet	53682	8.8.8.8	Internet	53	–	–	–	–	–
9	2024-10-22 09:48...	DNS Logs	–	10.5.42.89	–	Internet	53682	8.8.8.8	Internet	53	–	–	–	–	–
	2024-10-22 09:48...	DNS Logs	–	10.5.43.10	–	Internet	62542	114.144.114.114	Internet	53	–	–	–	–	–

Fig. 8. Real-time data indexing and retrieval

Customizability: To meet the needs of different enterprises and organizations, the system allows users to customize the interface according to the security areas they are concerned about, such as monitoring specific devices or specific attack types. Users can flexibly set different warning conditions based on network conditions to obtain targeted protection measures. User feedback shows that this feature improves the practicality and flexibility of the system.

Response time and ease of operation: Another point of concern in user feedback is the system's response time when generating alerts and handling events. Tests show that the system is able to generate alerts within seconds of detecting threats and immediately execute preset protective measures, such as blocking suspicious IP addresses or blocking attack paths. In actual operation, users believe that the system can respond to emergencies quickly without cumbersome manual intervention.

4.4 System Optimization Strategy

The system has been optimized to enhance stability, response speed, and accuracy based on testing and user feedback. Key optimizations include:

Model Optimization: The system regularly updates training data and employs feature selection, dimensionality reduction, and Ensemble Learning, combining multiple model predictions to improve detection accuracy and stability while reducing computational load.

Resource Management and Allocation: Dynamic resource allocation adjusts processing nodes based on network traffic, preventing bottlenecks during peak loads. Load balancing distributes tasks evenly to avoid overloading any single node.

System Monitoring and Log Analysis: An internal monitoring module tracks performance and resource usage in real time, automatically adjusting resources when performance declines. Detailed log analysis

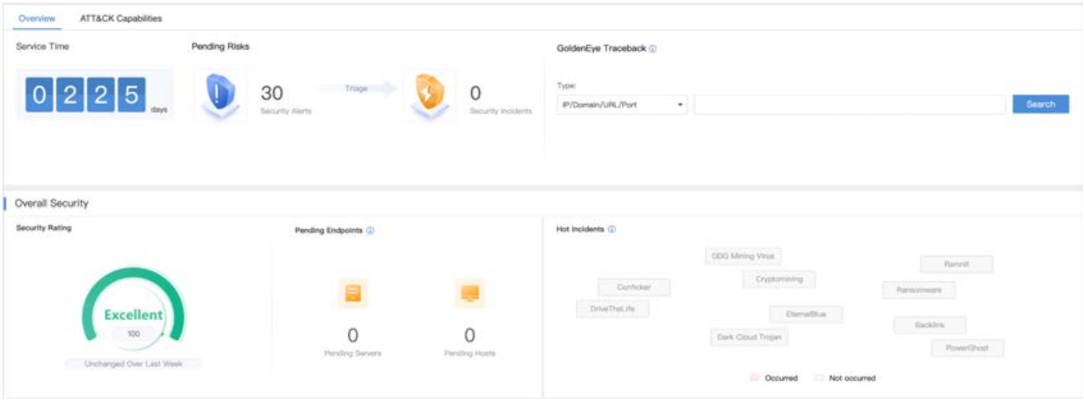
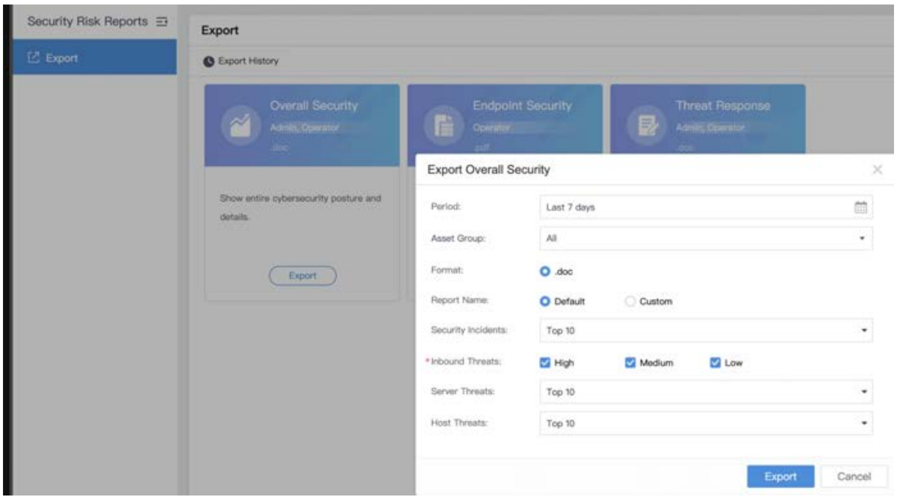


Fig. 9. Network security threat information display overview diagram



Show entire cybersecurity posture and details.

Export Overall Security

Period: Last 7 days

Asset Group: All

Format: ● .doc

Report Name: ● Default ○ Custom

Security Incidents: Top 10

*Inbound Threats: ☑ High ☑ Medium ☑ Low

Server Threats: Top 10

Host Threats: Top 10

Fig. 10. Security Risk Reports

provides insights into system status, enhancing stability and guiding further optimizations.

Conclusions. This research presents a situational awareness system that enhances network threat detection and response capabilities for SMEs. By integrating multi-source log data and leveraging advanced machine learning algorithms, the system delivers accurate and timely detection of complex threats. The user-friendly interface ensures accessibility for non-professional users, enabling SMEs to manage network security effectively and proactively. Experimental results demonstrate the system's scalability, processing large-scale log data efficiently and reducing security incident frequency and impact.

Future Prospects. The study identifies several areas for future research:

Incorporation of Deep Learning: Future iterations of the system could leverage deep learning to improve the detection of advanced persistent threats (APTs) and adapt to evolving attack patterns more effectively [9, p. 2].

Privacy Protection and Compliance: As data privacy becomes more critical, future work should focus on integrating privacy-preserving techniques, such as Federated Learning, while ensuring compliance with GDPR, CCPA, and other data privacy regulations [10, p. 108].

Scalability and Adaptability: To accommodate larger networks and multi-data center architectures, the system's scalability should be enhanced. Future research could explore strategies to balance localized and global threat detection capabilities in complex environments.

Bibliography:

1. Y. He. Research on the Key Technology of Network Security Based on Machine Learning. *2021 6th International Conference on Intelligent Computing and Signal Processing (ICSP)*, Xi'an, 2021. P. 972-975. DOI: 10.1109/ICSP51882.2021.9408756.

2. Z. Yifan, Application of Machine Learning in Network Security Situational Awareness, *2021 World Conference on Computing and Communication Technologies (WCCCT)*, Dalian, 2021. P. 39-46, DOI: 10.1109/WCCCT52091.2021.00015.

3. Y. Zhong, S. Wang, Research and Design of Visual Analytics System of Network Security Situation Based on Multi-source Log, *2020 7th International Conference on Information Science and Control Engineering (ICISCE)*, Changsha, 2020. P. 1095-1099, DOI: 10.1109/ICISCE50968.2020.00223.

4. A. Benzekri, R. Laborde, A. Oglaza, D. Rammal and F. Barrère, Dynamic security management driven by situations: An exploratory analysis of logs for the identification of security situations, *2019 3rd Cyber Security in Networking Conference (CSNet)*, Quito, 2019. P. 66-72, DOI: 10.1109/CSNet47905.2019.9108976.

5. H. Tao, J. Zhou, S. Liu, A survey of network security situation awareness in power monitoring system, *2017 IEEE Conference on Energy Internet and Energy System Integration (EI2)*, Beijing, 2017. P. 1-3, DOI: 10.1109/EI2.2017.8245487.

6. M. Wurzenberger, G. Höld, M. Landauer, F. Skopik. Analysis of statistical properties of variables in log data for advanced anomaly detection in cyber security. Computers & Security, 2023. V. 137.

7. E. Novikova and I. Kotenko, Analytical Visualization Techniques for Security Information and Event Management, *2013 21st Euromicro International Conference on Parallel, Distributed, and Network-Based Processing*, Belfast, 2013. P. 519-525, DOI: 10.1109/PDP.2013.84.

8. I. Sharafaldin, A. Habibi Lashkari, Ali A. Ghorbani. An Evaluation Framework For Network Security Visualizations. Computers & Security. Computers & Security, 2019. V. 84, P. 70-92, DOI:10.1016/j.cose.2019.03.005.

9. S. S. Karim, M. Afzal, W. Iqbal, D. Al Abri. Advanced Persistent Threat (APT) and intrusion detection evaluation dataset for Linux systems 2024. Data in Brief, 2024. V. 54, DOI: 10.1016/j.dib.2024.110290.

10. Y. -S. Martin, A. Kung, Methods and Tools for GDPR Compliance Through Privacy and Data Protection Engineering, *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, London, 2018, P. 108-111, DOI: 10.1109/EuroSPW.2018.00021.

Фу Бінь, Сарнацький В.В. РОЗРОБКА ТА ВПРОВАДЖЕННЯ СИСТЕМИ СИТУАЦІЙНОЇ ОБІЗНАНОСТІ НА ОСНОВІ АНАЛІЗУ ЖУРНАЛІВ БЕЗПЕКИ З ДЕКІЛЬКОХ ДЖЕРЕЛ

Стаття присвячена розробці та впровадженню інноваційної системи ситуаційної обізнаності на основі аналізу журналів безпеки з декількох джерел, орієнтованої на малі та середні підприємства (МСП), які стикаються з проблемами кібербезпеки. Виявлено, що МСП через обмежені ресурси та відсутність спеціалізованого персоналу з безпеки є особливо вразливими до нових кіберзагроз. У статті представлено систему, яка інтегрує дані журналів з декількох джерел безпеки в мережі, таких як брандмауери, системи виявлення вторгнень (IDS) та брандмауери веб-додатків (WAF), використовуючи обробку даних у режимі реального часу та методи машинного навчання для підвищення точності *виявлення загроз. Система використовує передові алгоритми для виявлення потенційних інцидентів безпеки та зменшення кількості помилкових спрацьовувань, забезпечуючи таким чином більш надійні оповіщення. Зазначається, що зручний інтерфейс системи спрощує складні дані про безпеку, роблячи їх доступними для непрофесійних користувачів, і дозволяє їм вживати проактивних заходів у відповідь на потенційні загрози.*

У статті також підкреслюється масштабованість системи, яка дозволяє їй адаптуватися до різних розмірів організацій і середовищ загроз, що робить її придатною як для малих підприємств з мінімальними ресурсами, так і для більших організацій з більш складними потребами в безпеці. Дослідження підкреслює важливість доступних, інтелектуальних рішень у сфері безпеки для подолання прогалин у кібербезпеці малих і середніх підприємств, які дозволяють їм виявляти, оцінювати та зменшувати загрози з більшою швидкістю та точністю, як це роблять великі підприємства зі спеціалізованими командами безпеки. Крім того, система розроблена для роботи в режимі реального часу, обробляючи великі обсяги різнорідних даних журналів, забезпечуючи при цьому високу продуктивність системи без шкоди для точності.

На додаток до основного акценту на зручність використання і масштабованість, в статті розглядаються ключові проблеми інтеграції журналів безпеки з різних джерел, підвищення швидкості і точності виявлення загроз, а також забезпечення швидкої реакції системи в умовах високих робочих навантажень. Пропонуючи практичне рішення для МСП, це дослідження робить свій внесок у постійні зусилля з демократизації кібербезпеки, надаючи невеликим організаціям інструменти, необхідні для захисту від все більш витончених кібератак.

Ключові слова: *Ситуаційна обізнаність, багатоджерельні журнали безпеки, машинне навчання, візуалізація даних, обробка в реальному часі, кібербезпека.*