Integration of Vulnerability Databases into ISMS: A Path to Enhancing Cyber Resilience of Critical Systems

Valentyna Yashchuk[1,†], Andriy Ivanusa[1,†], Nataliya Maslova[1,2,*,†], Rostyslav Tkachuk[1,3,†]

[1] *Lviv State University of Life Safety, 35, Kleparivska St., Lviv, 79007, Ukraine*

[2] *Donetsk National Technical University, 76, Sambirska, St., Drohobych, Lviv region, 82100, Ukraine*

[3] *Lviv Polytechnic National University, 12 Stepana Bandery str., 79013, Lviv, Ukraine*

Abstract

This article addresses the integration of vulnerability databases into Information Security Management Systems (ISMS) to enhance the cyber resilience of critical systems. The relevance of the problem is driven by the growing intensity of cyberattacks, the shrinking window between vulnerability disclosure and exploitation, and the increasing complexity of cloud and OT/ICS environments. Traditional vulnerability management remains fragmented, relies on manual prioritization, and lacks timely correlation between technical attributes and business risks.

A conceptual model and methodological framework are proposed for embedding data from vulnerability databases (CVE/NVD, CISA KEV, CWE, and EPSS/First.org) into ISMS processes in alignment with ISO/IEC 27001/27002 and NIST recommendations. The approach includes automated collection and normalization of vulnerability records, contextual enrichment using CMDB, IAM, and EDR data, correlation with SIEM and SOAR systems, and risk-oriented prioritization. The proposed model integrates CVSS severity, KEV status, EPSS probability, asset criticality, and exploit availability to support risk-oriented decision-making and response planning.

Case studies involving CVE-2021-44228 (Log4Shell) and CVE-2023-23397 (Microsoft Outlook) illustrate the transformation of vulnerability intelligence into practical security measures, including SOAR playbooks, ITSM-driven change management, automated patch deployment, and residual risk monitoring within the ISCM framework. The analysis suggests the potential for reducing mean time to detect (MTTD) and mean time to recover (MTTR), while improving compliance outcomes. Identified limitations include asset inventory quality, data inconsistencies, and operational constraints specific to OT/ICS environments. Future research directions involve machine learning-based exploitation prediction, DevSecOps integration, and cyber threat intelligence exchange through STIX/TAXII mechanisms. The proposed framework provides methodological and architectural foundations for implementing integrated vulnerability management and enhancing cyber resilience in critical infrastructure environments.

Keywords

Vulnerability Databases, ISMS, Cyber Resilience, Critical Infrastructure, Risk-Oriented Prioritization 1

1. Introduction

In today's digital world, information technologies are a fundamental component of the functioning of governmental, commercial, and social structures. However, their widespread adoption is accompanied by a rapid increase in cyber threats that can have critical consequences for national security and economic stability. Critical infrastructure—such as energy systems, transportation networks, communication systems, and governmental information resources—is particularly vulnerable.

Cyber threats can disrupt the operation of these systems, potentially causing large-scale failures, loss of confidential data, and economic imbalance. Vulnerabilities in information systems remain

[1]*RS-2026: Resilient Systems: Secure Digital Technologies and Critical Infrastructure, June 30, 2026, Drohobych, Ukraine*

* Corresponding author.

† These authors contributed equally.

v.yaschuk@ldubgd.edu.ua (V. Yashchuk); ivaaanusa@gmail.com (A. Ivanusa); masgpp2@gmail.com (N. Maslova); rlvtk@ukr.net (R. Tkachuk)

0000-0003-2651-4918 (V. Yashchuk); 0000-0001-9141-8039 (A. Ivanusa); 0000-0002-9078-0973 (N. Maslova); 0000-0001-9137-1891 (R. Tkachuk)

primary entry points for attackers, and delayed response significantly increases the risk of successful exploitation.

The integration of vulnerability data into Information Security Management Systems (ISMS) for critical assets has become strategically important. A key aspect is the use of modern vulnerability databases, which contain standardized information on known threats and potential exploitation scenarios. Integrating vulnerability data into ISMS enables timely threat identification, risk assessment, and automated response.

The aim of this work is to study methodological approaches for developing a conceptual model for integrating vulnerability databases (VDBs) into ISMS. Its application is demonstrated to reduce detection and response times and to lower the risk of successful exploitation of critical vulnerabilities, thereby enhancing the cyber resilience of critical infrastructure systems. To achieve this goal, the following tasks were defined:

1. Identify and systematize relevant vulnerability data sources;
2. Design the data and process architecture covering the workflow from collection and normalization to automated response;
3. Develop a prioritization model combining CVSS, EPSS, and KEV with asset criticality;
4. Define SOAR playbooks for automated responses and integration with monitoring and security systems of critical assets;
5. Determine performance metrics (MTTD, MTTR, KEV closure rate (%), and patch SLA compliance) and demonstrate the model on practical case studies.

The research object comprises the processes of ensuring information and cyber security of critical systems within ISMS. The research subject is the methodological and technological foundations for integrating vulnerability databases of various formats (CVE, NVD, CISA KEV, etc.) into ISMS to enhance the cyber resilience of critical systems.

The scientific novelty of this study lies in the integration of standardized exploitability metrics (CVSS/EPSS/KEV) with the business context of assets (CMDB, IAM) into a unified prioritization scoring framework, which is then linked to automated SOAR playbooks and ISCM policies.

Unlike traditional vulnerability management approaches that rely primarily on CVSS severity ratings and manual prioritization procedures, the proposed model combines exploitability prediction (EPSS), evidence of active exploitation (KEV), and business context derived from CMDB and IAM systems within a unified risk-oriented prioritization framework. This integration enables more accurate vulnerability assessment and supports automated decision-making within SIEM, SOAR, and ISMS processes.

2. Problem Description

The integration of vulnerability databases (VDBs) into Information Security Management Systems (ISMS) is a key factor in enhancing the cyber resilience of critical systems. Critical infrastructure—such as energy systems, transportation networks, healthcare information systems, and government services—is particularly vulnerable to cyber threats, as its availability and integrity directly impact national security and societal functioning.

Firstly, integration with global databases such as CVE (Common Vulnerabilities and Exposures), NVD (National Vulnerability Database), and CISA KEV enables timely access to up-to-date information on known vulnerabilities. This reduces the time between vulnerability disclosure and remediation, lowering the likelihood of real-time exploitation of critical assets.

Secondly, through data normalization and automated correlation with organizational assets, it becomes possible to identify which systems are at risk. For critical infrastructure, this allows precise prioritization of efforts on the most important components, such as SCADA systems or energy grid control gateways.

Thirdly, the use of integrated sources containing risk metrics (e.g., CVSS v3.1/v4.0 for severity assessment, EPSS for exploitation probability) enables effective security prioritization. This is

particularly crucial under limited resources, ensuring that mitigation efforts target the most dangerous vulnerabilities.

Fourthly, integration with ISMS supports the automation of management processes, including risk mitigation planning, incident management via SOAR solutions, and audit/reporting preparation. For critical infrastructure, this enhances system resilience while ensuring compliance with international security standards (ISO/IEC 27001, NIST CSF).

Currently, the main challenges include the increasing number of vulnerabilities, insufficient automation in detection, and limited capacity for timely risk assessment. Although ISO/IEC 27001 and NIST CSF provide a process framework for vulnerability management, they do not specify detailed integration with external sources. According to IBM X-Force and ENISA, over 60% of successful attacks on critical infrastructure exploit known vulnerabilities that were not timely addressed. This highlights the need for conceptual models formalizing the processes of collection, normalization, prioritization, and response within critical systems.

The growing dependence of essential services on ICT amplifies the frequency of cyberattacks. Vulnerability disclosures are continuous, while the "time to exploitation" is shrinking, creating a gap between detection and remediation. The practical effectiveness of ISMS depends on the ability to rapidly integrate external knowledge sources, particularly VDBs, into everyday monitoring, response, and change management cycles.

3. Literature Review

The review of the current state of research and the regulatory framework in the field of vulnerability management demonstrates the existence of established international standards and methodological documents that form the basis for building information security management systems (ISMS). In particular, the ISO/IEC 27001:2022 [1] and ISO/IEC 27002:2022 [2] standards define requirements for the creation, implementation, and improvement of ISMS, as well as provide practical recommendations for applying security measures.

Documents from the U.S. National Institute of Standards and Technology (NIST) detail specific aspects of security. In particular:

- NIST SP 800-61 Rev. 3 regulates incident management processes [3];
- NIST SP 800-40 Rev. 4 is dedicated to managing updates and patches [4];
- NIST SP 800-137 describes approaches to continuous security monitoring (ISCM) [5].

An important element of the regulatory ecosystem is the standardization of vulnerability assessment methods. CVSS v3.1/v4.0 (FIRST) provides a unified scale for assessing vulnerability severity. The CISA KEV catalog organizes known exploited vulnerabilities to prioritize their remediation. The EPSS model (FIRST) provides predictive estimates of the likelihood of exploitation [6,7]. Current scientific and industry research focuses on:

- The evolution of SIEM and SOAR technologies;
- Integration of vulnerability databases with system telemetry;
- The use of risk-based approaches for prioritization (combining CVSS, EPSS, and KEV);
- Automation of response via playbooks and their integration into DevSecOps processes, as discussed in recent studies on SIEM/SOAR evolution and AI-driven orchestration [8—11].

According to ENISA Threat Landscape 2023/2024 reports [12,13], special attention is paid to the role of known exploited vulnerabilities in modern cyberattack chains, highlighting the importance of their timely detection and mitigation.

At the same time, there are several challenges for effectively integrating vulnerability data into ISMS. Key issues include Heterogeneous information sources (CVE, NVD, KEV), Incomplete inventory of organizational assets, Difficulties in unifying software names (CPE), The need for accurate mapping of data to specific versions and hosts [14].

Additional barriers include high noise levels in SIEM systems and restrictions on patch deployment in operational technology (OT) environments and industrial control systems (ICS), where maintaining process continuity is critical.

Systematic information security management covers the entire lifecycle of protecting an organization's information assets — from planning and implementation to continuous monitoring and improvement of protective measures. This approach is based on the integration of several complementary methodologies.

The process-based approach structures information security management as a set of interconnected procedures: risk identification, vulnerability analysis and classification, planning of protective measures, their implementation, and subsequent monitoring. This ensures decision formalization and a sequence of actions within the system.

The risk-based approach focuses on risk assessment, enabling prioritization of resources to protect the most critical assets and concentrate on the most dangerous attack vectors. This model is particularly important for critical IT systems, where even minor vulnerabilities can have significant consequences.

The standardized approach ensures compliance with international norms: ISO/IEC 27001, ISO/IEC 27005, NIST CSF, COBIT, ITIL [1—7, 12—14]. These standards provide unified requirements for vulnerability detection, classification, and handling processes, as well as describe requirements for policies, procedures, and technical solutions.

The adaptive approach allows the security system to respond quickly to changes — new cyber threats, vulnerabilities, regulatory updates, or changes in the architecture of the information system. Flexibility is ensured through regular review of strategies, procedures, and technologies, along with the implementation of dynamic risk analysis.

Thus, effective information security management requires combining different methodological approaches adapted to the organization's specifics. The combination of process-based, risk-based, systemic, standardized, and adaptive approaches creates a resilient, flexible, and effective ISMS capable of countering modern cyber threats and ensuring business continuity.

The methodological basis of the study is a comprehensive analysis of scientific sources dedicated to the use of intelligent methods and modern technologies in protecting critical information infrastructure. A systematic literature review was conducted, covering both fundamental theoretical developments and practical aspects of implementing modern cybersecurity approaches [8-11, 15-24].

Special attention is paid to the comparative analysis of contemporary researchers' concepts, allowing the identification of key trends, development prospects, and potential directions for improving existing security systems [25-32].

Modern vulnerability databases are centralized platforms that collect, systematize, and publish information about discovered vulnerabilities in software, hardware, and networks. They are critically important for cybersecurity specialists as they allow rapid response to new threats, risk assessment for systems, and prioritization of updates and remediation measures.

Research on vulnerability database reviews [33—38] focuses on methods of vulnerability classification and categorization, tools for automated vulnerability detection integrated with databases, evaluation of the effectiveness of security measures recommended in the databases and their impact on threats to information systems.

In the previous research phase [17, 30—32], the authors conducted a detailed comparative analysis of leading vulnerability databases (NVD, CVE® MITRE, CISA KEV, Microsoft SUG, VulnDB, OSV, IBM X-Force, CERT). The analysis covered key parameters: support for CVE, CVSS, CWE standards; availability of open APIs; export formats (CSV, JSON, XML); and potential for ISMS integration.

The analysis presented in [17] demonstrated that no single vulnerability database fully covers all functions required for comprehensive risk assessment. Instead, the combined use of multiple sources improves the completeness of vulnerability intelligence and supports more effective diagnostics and response processes. The present study extends the results reported in our previous work [17], where a general conceptual framework for integrating vulnerability databases into Information Security Management Systems (ISMS) was introduced. Unlike [17], which primarily focused on the role of vulnerability intelligence in improving cyber resilience, this paper develops a detailed integration architecture, formalizes risk-oriented prioritization mechanisms based on CVSS, EPSS, KEV, and asset criticality, and proposes practical implementation scenarios involving SIEM, SOAR, CMDB,

IAM, ITSM, and ISCM components. Thus, the current work represents a methodological and architectural extension of the previously proposed concept.These findings formed the basis for developing a structural model of an integrated system. The model implements sequential integration of data from external vulnerability databases at all stages: from aggregation and normalization to risk prioritization and automated response. The model provides a practical mechanism for implementing vulnerability management in critical IT systems.

For information integration, various sources, systems, and methods were used. The main sources were public and verified databases: CVE (Common Vulnerabilities and Exposures) and NVD (National Vulnerability Database), which contain descriptors, CPE (Common Platform Enumeration) identifiers, and CVSS (Common Vulnerability Scoring System) metrics. For prioritization, the CISA KEV (Known Exploited Vulnerabilities) catalog was applied. Weakness classification was performed using CWE (Common Weakness Enumeration), and the likelihood of exploitation was evaluated using the EPSS (Exploit Prediction Scoring System) model. Vendor security bulletins containing patch releases and manufacturer recommendations were also considered.

Various information systems were applied for comprehensive integration:

1. SIEM — for centralization and correlation of telemetry;
2. SOAR — for automated response;
3. CMDB — for accounting for asset criticality and dependency on vulnerabilities;
4. IAM — for assessing identity-related risks;
5. EDR/NDR — for integrating endpoint and network signals;
6. ITSM platforms (ServiceNow, Jira Service Management) — for managing incident and change lifecycles.

The methodology included normalization and unification of data formats (JSON from NVD and CISA), mapping CPE identifiers to actually installed packages using vulnerability scanners and SBOMs. Correlation of vulnerability data with events recorded in SIEM allowed detection of critical incidents. Prioritization was performed using a risk-based scoring model combining CVSS, KEV, and EPSS. Additionally, process metrics such as Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), and SLA compliance were evaluated to assess the effectiveness of the integrated approach.

4. Results

The research results demonstrated that the integration of vulnerability databases into ISMS creates added value in the context of ensuring the cyber resilience of critical systems. This approach enables not only the timely identification of weaknesses in information resources but also the effective prioritization of mitigation measures based on actual risks. The general workflow of transforming vulnerability intelligence into risk-oriented decisions is presented in Figure 1.

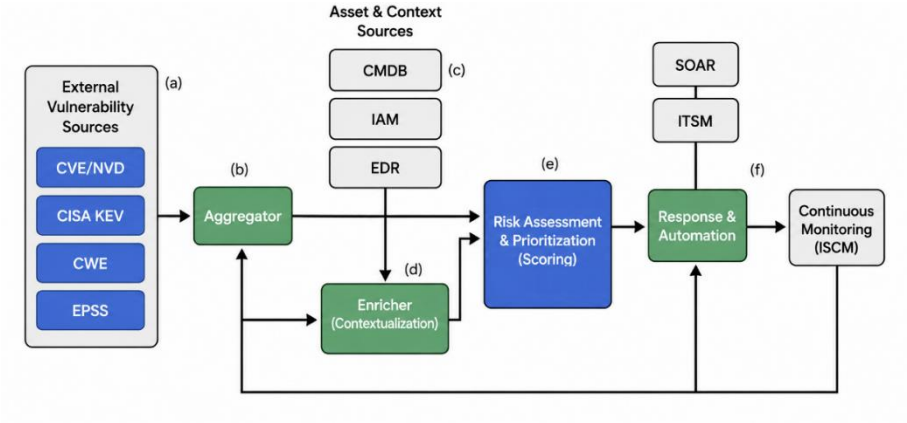

Figure 1. Conceptual Framework for Risk-Oriented Integration of Vulnerability Intelligence into ISMS

Figure 1 presents the conceptual workflow of vulnerability intelligence integration within the ISMS, including aggregation, contextualization, risk prioritization, response automation, and continuous monitoring. The feedback loop emphasizes the adaptive nature of the proposed framework and its contribution to cyber resilience of critical systems.

Three main scenarios reflecting the practical implementation of the concept were identified during the study:

1. Reactive scenario. SIEM and SOAR systems receive data from CVE/NVD and KEV in real time. Detected incidents are automatically enriched with information about known vulnerabilities, after which appropriate response playbooks are generated. This scenario reduces MTTD and MTTR but has limitations in predicting future threats.
2. Proactive scenario. The use of EPSS models combined with CVSS and KEV allows assessing not only the severity of vulnerabilities but also the likelihood of their exploitation. This enables the development of risk-oriented patch management strategies and prioritization of assets in CMDB according to their criticality.
3. Predictive scenario. The integration of vulnerability databases with DevSecOps practices and SBOM facilitates early detection of weaknesses at the development and testing stages. Integration with EDR/NDR makes it possible to simulate attacks and verify the effectiveness of applied countermeasures in near real-time.

The final outcome of the study was the development of a conceptual framework for integrating vulnerability intelligence into Information Security Management Systems (ISMS), which forms the basis for the proposed risk-oriented vulnerability management process.

A distinctive feature of the proposed framework is the integration of exploitability metrics (EPSS), evidence of active exploitation (KEV), and organizational asset context into a unified risk assessment process. This enables more accurate prioritization of vulnerabilities than approaches relying solely on CVSS severity ratings and supports automated risk treatment decisions within the ISMS lifecycle.

The use of modern vulnerability databases within such a system allows for the rapid identification of vulnerabilities in digital infrastructure; reduces response times to critical incidents; optimizes resource allocation by focusing on the most significant risks; automates security audits; and ensures compliance with international requirements and standards.

Thus, the combination of process-oriented, risk-based, adaptive, and standardized approaches forms the foundation of a reliable, dynamic, and scalable information security management system, which is especially critical for the protection of strategically important infrastructure.

In this work, unlike previous studies by the authors [17, 31–33], the CERT database is not included in the generalized list of integrated system components. This is due to the fact that the CERT database lacks extensive integration capabilities via API or in JSON/XML formats, unlike other sources (NVD, VulnDB, Microsoft SUG, OSV, etc.). Its content is published as notes primarily intended for human reading rather than machine processing. Therefore, for automated, scalable implementation of an integrated risk management system, CERT has limited practical application in the context of real-time monitoring.

The practical realization of this conceptual framework requires the integration of vulnerability intelligence sources with organizational monitoring, response, and governance mechanisms.

The proposed conceptual model for integrating vulnerability databases can be implemented within automated monitoring and information security management systems for critical infrastructure assets, such as energy complexes, transportation hubs, or government information systems.

In the context of Ukraine, the proposed framework can also be applied to information and communication systems of the State Emergency Service of Ukraine (SESU), including emergency notification, situational awareness, and crisis management systems, where timely vulnerability identification and response are essential for maintaining the continuity of civil protection functions.

Practical implementation of the model should include the following stages:

1. Connecting vulnerability sources (e.g., NVD, VulnDB, OSV) to the event collection system via API or uploading in a unified JSON/XML format;

2. Aggregation and processing of information using a server-side module that normalizes data, adds risk assessments (CVSS, EPSS), and marks the presence of exploits;
3. Contextualization of vulnerabilities by mapping them to organizational assets in the CMDB, enabling the determination of the criticality of each vulnerability;
4. Transmitting analysis results to SIEM or SOAR systems, which generate automated response playbooks, such as blocking network activity, creating incidents, and notifying administrators;
5. Monitoring the implementation of measures and reassessing residual risk, enabling continuous real-time improvement of security policies.

The practical implementation stages are reflected in the reference architecture shown in Figure 2, which presents the technical integration of vulnerability databases with organizational monitoring, response, and governance systems. The architecture organizes the process as a sequence of functional flows, including data ingestion from vulnerability databases, normalization and contextual enrichment through CMDB, IAM, and EDR integration, event correlation within SIEM, risk-based prioritization, automated response via SOAR playbooks, ITSM-driven change management, and continuous residual risk monitoring within the ISCM framework.

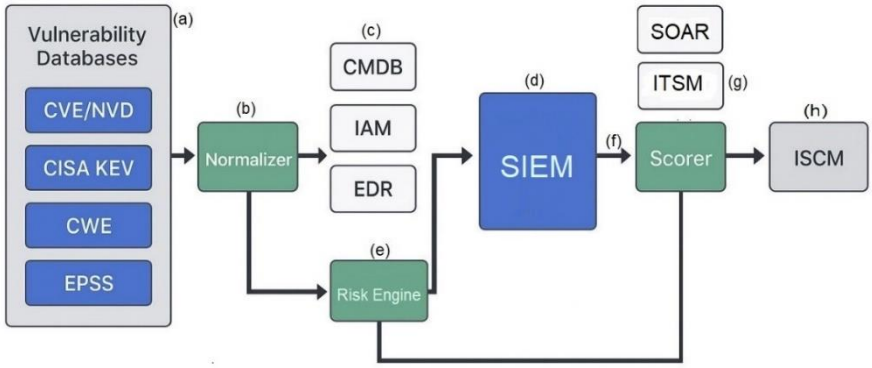

Figure 2. Reference Architecture for VDB Integration within the ISMS

This architecture supports a continuous cycle of vulnerability assessment and mitigation and provides the basis for automated, risk-oriented decision-making. The corresponding processing pipeline consists of seven functional modules: Ingest, Normalizer, Resolver, Enricher, Scorer, Actioner, and Metrics, which collectively enable the sequential acquisition, contextualization, prioritization, and response to vulnerability intelligence.

To support risk-oriented prioritization, the proposed framework calculates an integrated risk score for each vulnerability by combining severity, exploitability, evidence of active exploitation, asset criticality, and exploit availability. The overall risk score (R_i) for a specific vulnerability is determined as follows:

$$R_i = w_1 \cdot CVSS_i + w_2 \cdot EPSS_i + w_3 \cdot KEV_i + w_4 \cdot CritAsset_i + w_5 \cdot ExploitAvail_i$$

where

w_k — weighting coefficients configured according to the organization's policies;

$CVSS_i$ — CVSS severity score of vulnerability i;

$EPSS_i$ — EPSS probability score of vulnerability i;

$KEV_i \in \{0,1\}$— binary indicator of whether vulnerability i is included in the CISA Known Exploited Vulnerabilities (KEV) catalog;

$CritAsset_i$ — criticality score of the asset based on CMDB data;

$ExploitAvail_i$ — indicator of the availability of public exploits or involvement in widespread campaigns.

The calculated risk values are compared against predefined thresholds to classify vulnerabilities according to priority levels (P1–P4) and establish corresponding SLA targets for incident handling.

This scoring model links vulnerability intelligence with organizational context and enables automated prioritization and response planning.

The workflows for vulnerability response and mechanisms for controlling the execution of mitigation measures are as follows. For the highest-priority vulnerabilities (P1 — presence in KEV, high EPSS, critical asset), comprehensive measures are applied: automated isolation or blocking via SOAR, emergency patch deployment or implementation of compensating controls, enhanced signature monitoring in SIEM and EDR, as well as mandatory post-incident investigation. Vulnerabilities of P2—P3 priority are addressed through planned procedures: scheduled patching, task tracking via ITSM tickets, and regular reporting on mitigation progress. The lowest-priority vulnerabilities (P4) are either accepted as residual risk or addressed later, with periodic monitoring of residual risk within the ISCM framework. This approach ensures a systematic and differentiated response to vulnerabilities based on their criticality and likelihood of exploitation, supporting effective risk management within the organization's information infrastructure.

Let us consider two examples of applying the proposed approach (Table 1).

Table 1
Integrated approach to vulnerability management

Case	VDB data	Prioritization (model)	SOAR / EDR / WAF	SIEM / Analytics	ITSM / Changes	ISCM/Risk Control
CVE-2021-44228 (Log4Shell)	CVSS: critical; widespread exploitation; KEV: present	P1 (high EPSS + KEV)	Log4j scanning, WAF, JNDI blocking, prioritized patching, compensating controls	Correlation of HTTP logs with Threat Intelligence sources	Change planning and maintenance windows	Residual risk monitoring after response
CVE-2023-23397 (Microsoft Outlook)	Privileged escalation via crafted reminder (KEV present)	P1 for mail servers/critical workstations	Blocking IoCs in EDR/Proxy and enforcing software updates	Targeted analytic rules for early attack detection	Access audit control	Monitoring residual risk and the effectiveness of measures

Table 1 illustrates a comprehensive approach to vulnerability management, where each case is assessed using VDB, prioritized according to the integrated risk model, and subsequently subjected to automated, analytical, and procedural mitigation measures.

The first example is CVE-2021-44228 (Log4Shell), characterized by a critical CVSS score, widespread exploitation, and inclusion in the CISA KEV catalog. Based on high EPSS values and KEV presence, the vulnerability is classified as a P1 risk. Automated response mechanisms include identification of vulnerable Log4j components, prioritized patch deployment, and implementation of compensating controls via SOAR workflows. The second example is CVE-2023-23397, associated with privilege escalation in Microsoft Outlook and also included in the KEV catalog. For critical workstations and mail servers, the model assigns a P1 priority. Response measures involve automated software updates and blocking of compromise indicators through integrated EDR mechanisms and security monitoring tools

Both cases demonstrate the effectiveness of an integrated approach to vulnerability management, combining automated response mechanisms, event correlation, scheduled changes, and systematic residual risk control. This approach significantly reduces the likelihood of exploitation of critical vulnerabilities and optimizes the organization's information security resources.

5. Discussion

The obtained results demonstrate that integrating vulnerability databases into an Information Security Management System (ISMS) directly contributes to increasing the cyber resilience of critical systems. By accelerating the detection and mitigation of vulnerabilities, organizations reduce their attack surface and maintain operational continuity even under active cyberattacks. This approach is particularly important for critical infrastructure sectors such as energy, transportation, telecommunications, and finance, where system failures or compromises could lead to catastrophic consequences.

The obtained results indicate that the implementation of an integrated approach may provide the following benefits:

- Reduction of "noise" in SIEM through contextualization of events using KEV and EPSS;
- Improved accuracy in detecting critical incidents due to correlation with CMDB data;
- Optimization of resource usage through prioritization of the most dangerous vulnerabilities;
- Reduced risks for monitoring and control systems of operational technologies and industrial control systems (OT/ICS) thanks to forecasting of potential exploitation scenarios, which is critically important under limited patching capabilities.

The effectiveness of the proposed approach is evaluated using the following metrics: mean time to detect an incident (MTTD), mean time to recover after an incident (MTTR), the proportion of closed vulnerabilities from the CISA Known Exploited Vulnerabilities (KEV) list within a given period, the percentage of assets affected by critical CVEs, compliance with established SLAs for patch deployment, and the dynamics of incident volume related to known exploited vulnerabilities.

Expected outcomes from implementing this approach include a reduction in MTTD and MTTR through automated response processes and playbook execution, an increased share of timely remediated KEVs, a decrease in incidents exploiting known exploits, and improved audit results in accordance with ISO and NIST standards.

The proposed approach provides an integrated, risk-oriented security management mechanism aligned with the ISMS. Automating the process from detecting vulnerabilities in databases (VDBs) to implementing corresponding measures enhances response speed. Moreover, the approach ensures verifiable compliance with established standards and enables transparent reporting.

Compared with traditional vulnerability management approaches that rely primarily on CVSS severity ratings and manual prioritization, the proposed framework incorporates exploitability prediction (EPSS), evidence of active exploitation (KEV), and organizational asset context derived from CMDB and IAM systems. This enables more accurate prioritization of remediation activities and improves the allocation of security resources in critical environments.

The effectiveness of the proposed framework may be influenced by several factors, including the completeness and quality of asset inventories maintained within CMDB repositories, ambiguities in software identification through CPE naming conventions, the presence of duplicate or inconsistent records, restricted maintenance windows, and operational constraints in OT/ICS environments that limit the timely deployment of security updates. Additional implementation challenges include heterogeneous data formats (JSON, XML, CSV), automated mapping of vulnerabilities to organizational assets, and the need to ensure the accuracy and timeliness of external vulnerability intelligence sources.

The use of KEV and EPSS also introduces certain limitations. The KEV catalog contains only vulnerabilities for which active exploitation has already been confirmed and therefore may not provide early visibility into emerging threats. Similarly, EPSS produces probabilistic estimates of exploitation likelihood rather than deterministic predictions. Consequently, KEV and EPSS should be considered complementary decision-support mechanisms rather than standalone indicators of cyber risk.

These limitations can be mitigated through improved asset management practices, the adoption of Software Bills of Materials (SBOMs), software name normalization procedures, regular validation of asset inventories, and the implementation of compensating security controls such as network

segmentation, web application firewalls (WAFs), access control policies, partial isolation of critical services, and virtualization technologies.

The conducted study allowed for the formulation of practical recommendations for implementation:

- Align asset directories (CMDB) with CPE and SBOM to ensure accurate component identification;
- Configure regular automated ingestion of data from NVD, KEV, and EPSS to maintain up-to-date vulnerability information;
- Harmonize risk scoring weights (R) with internal risk management policies;
- Develop a minimal set of SOAR playbooks for handling P1/P2 incident categories;
- Integrate ITSM processes to propagate security-related changes;
- Implement ISCM dashboards for management to monitor the effectiveness of security measures;
- Introduce CVE-check gates in DevSecOps CI/CD pipelines for early detection and remediation of vulnerabilities.

6. Conclusions

The study examines a conceptual approach to building an integrated system for risk modeling and management in critical information-technical systems through the use of vulnerability databases. The research achieved the following results:

1. Relevant sources of vulnerability data were identified, including NVD, CVE, CISA KEV, IBM X-Force, VulnDB, and OSV, which provide standardized information suitable for automated analysis and integration. It was noted that the CERT database was not included in the generalized list of integrated system components, as it lacks broad integration capabilities via API or in JSON/XML formats.
2. A conceptual framework and reference integration architecture were developed, covering data aggregation, normalization, contextualization, risk prioritization, and integration with ISMS, SIEM, and SOAR systems.
3. The application of the model in monitoring and protection systems for critical infrastructure was substantiated, particularly in energy, transportation, and governmental IT infrastructures, where timely response to vulnerabilities is essential to ensure continuous operation.

The proposed system enhances risk management efficiency, reduces response time to threats, optimizes resources, and complies with international security standards. The model provides a comprehensive information processing cycle—from data collection to automated response—adheres to international standards, and is adapted for integration into the infrastructure of critical assets. Its implementation represents a crucial step toward ensuring the cyber resilience of critical infrastructure.

The integration of vulnerability databases (VDB) into an Information Security Management System (ISMS) transforms the protection model for critical systems from reactive to proactive. The proposed architecture, combined with risk-oriented scoring that integrates CVSS, EPSS, KEV, and asset criticality, as well as the use of automated SOAR playbooks, enables the reduction of incident detection and response times, lowers the likelihood of successful exploitation of known vulnerabilities, and improves system compliance with established security standards. The model is technologically neutral, scalable, and suitable for implementation across various critical infrastructure sectors.

Further development of the concept can be pursued in the following directions:

- Applying machine learning methods to predict the likelihood of vulnerability exploitation and automatically adjust scoring weights;
- Correlating VDB data with behavioral models of users and assets (UEBA) and telemetry from EDR/NDR systems to improve risk assessment accuracy;

- Integrating with international and national cyber threat intelligence sharing frameworks (STIX/TAXII) and associated repositories;
- Developing specifications for compensating controls in OT/ICS systems, considering operational update constraints;
- Formalizing key performance indicators (KPI) and critical success factors (CSF) for audit assessment and enhancing transparency in security management.

Acknowledgements

We would like to express our sincere gratitude to all members of the research group whose dedicated and diligent work made a significant contribution to this study. We are also thankful to the staff of the Department of Information Security Management of the Lviv State University of Life Safety for their constructive ideas and professional recommendations, which significantly contributed to improving the presented results and facilitating their integration into the educational process.

Declaration on Generative AI

During the preparation of this work, the authors used ChatGPT (OpenAI) and Microsoft Copilot for grammar and spelling checks, improvement of academic writing style, preparation of preliminary figure schematics, and verification of the manuscript's compliance with CEUR requirements. The authors reviewed and edited all AI-generated suggestions and take full responsibility for the publication's content.

References

[1] International Organization for Standardization. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. ISO, 2022. URL: https://www.iso.org/standard/82875.html

[2] International Organization for Standardization. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls. ISO, 2022. URL: https://www.iso.org/standard/75652.html

[3] National Institute of Standards and Technology. Incident Response Recommendations and Considerations for Cybersecurity Risk Management (SP 800-61 Rev. 3). NIST, 2025. doi:10.6028/NIST.SP.800-61r3

[4] National Institute of Standards and Technology. Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology (SP 800-40 Rev. 4). NIST, 2022. doi:10.6028/NIST.SP.800-40r4

[5] National Institute of Standards and Technology. Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations (SP 800-137). NIST, 2011. doi:10.6028/NIST.SP.800-137

[6] Forum of Incident Response and Security Teams. Common Vulnerability Scoring System (CVSS) v4.0 Specification Document. FIRST, 2023. URL: https://www.first.org/cvss

[7] Forum of Incident Response and Security Teams. Exploit Prediction Scoring System (EPSS) User Guide. FIRST, 2023. URL: https://www.first.org/epss

[8] S. R. Pulyala. The future of SIEM in a machine learning—driven cybersecurity landscape. Turkish Journal of Computer and Mathematics Education, vol. 14, no. 3, 2023, pp. 1309—1314.

[9] S. Ramakrishnan, D. R. Chittibala. Enhancing cyber resilience: convergence of SIEM, SOAR, and AI in 2024. Int. J. Comput. Eng., vol. 5, no. 2, 2024, pp. 36—44. ISSN: 2958—7425.

[10] M. F. Ansari. The impact and limitations of artificial intelligence in cybersecurity: a literature review. Int. J. Adv. Res. Comput. Commun. Eng., 2022.

[11] U. M. Bartwal. Security orchestration, automation, and response engine for deployment of behavioural honeypots. In: Proceedings of the IEEE Conftrence Dependable and Secure Computing (DSC), 2022, pp. 1—8.

[12] European Union Agency for Cybersecurity. ENISA Threat Landscape 2023. ENISA, 2023. URL: https://www.enisa.europa.eu/publications
[13] European Union Agency for Cybersecurity. ENISA Threat Landscape 2024. ENISA, 2024. URL: https://www.enisa.europa.eu/publications
[14] Cybersecurity and Infrastructure Security Agency. Known Exploited Vulnerabilities Catalog. CISA, 2024. URL: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
[15] A. Aghazadeh Ardebili, M. Lezzi, M. Pourmadadkar. Risk assessment for cyber resilience of critical infrastructures: Methods, governance, and standards. Applied Sciences, vol. 14, no. 24, 2024, 11807. doi:10.3390/app142411807
[16]A. Longo, A. Aghazadeh Ardebili, A. Lazari, A. Ficarella. Cyber—physical resilience: Evolution of concept, indicators, and legal frameworks. Electronics, vol. 14, no. 8, 2025, 1684. doi:10.3390/electronics14081684
[17] V. Yashchuk, A. Ivanusa, N. Maslova, R. Tkachuk, T. Brych. Kontseptualizatsiia intehratyvnoho vykorystannia baz danykh vrazlyvostei u konteksti systemnoho menedzhmentu informatsiinoi bezpeky. Visnyk LDUBZhD, no. 31, 2025, pp. 126—139. doi:10.32447/20784643.31.2025.13
[18] W. S. Admass, Y. Y. Munaye, A. A. Diro. Cyber security: State of the art, challenges and future directions. Cyber Security and Applications, vol. 2, 2024, 100031. doi:10.1016/j.csa.2023.100031
[19] V. Tzavara, S. Vassiliadis. Tracing the evolution of cyber resilience: a historical and conceptual review. Int. J. Inf. Secur., vol. 23, 2024, pp. 1695—1719. doi:10.1007/s10207-023-00811-x
[20] O'Reilly Media. *Critical infrastructure security*. O'Reilly Media, 2023. URL: https://www.oreilly.com/library/view/critical-infrastructure-security/9781837635030/
[21] N. AlFardan. *Cyber threat hunting*. Manning Publications, 2025. ISBN: 978-1-63343-947-4.
[22] G. Blokdyk. *Cybersecurity education: A complete guide — 2024 edition*. 5STARCooks, 2024. ISBN: 978-1-03881-235-3.
[23] A. Evans. Enterprise cybersecurity in digital business: Building a cyber-resilient organization. Taylor & Francis, 2022. ISBN: 978-0-367-51149-4.
[24] M. Kofler, K. Gebeshuber et al. Hacking and security: The comprehensive guide to penetration testing and cybersecurity. Rheinwerk Computing, 2023. ISBN: 978-1-4932-2425-5.
[25] M. Küfeoğlu, S. Piccini, A. Foley. *Cyber resilience in critical infrastructure*. Routledge, London, 2024.
[26] A. Magnusson. Practical vulnerability management: A strategic approach to managing cyber risk. No Starch Press, San Francisco, CA, 2020.
[27] R. Setola, V. Rosato, S. Panzieri (Eds.). Critical infrastructure security and resilience: Theories, methods, tools, and technologies. Springer, Cham, 2020.
[28] G. Areo. Advancing cyber resilience through the convergence of SIEM, SOAR, and AI technologies. December 2023. URL: https://www.researchgate.net/publication/386674188
[29]N. Shimizu, M. Hashimoto. Vulnerability management chaining: an integrated framework for efficient cybersecurity risk prioritization. Preprint, Kagawa University, Japan, June 2025. DOI: https://doi.org/10.48550/arXiv.2506.01220
[30]V. Yashchuk. Rol ta mistse stratehii kiberbezpeky Ukrainy u zabezpechenni informatsiinoi bezpeky derzhavy. In: Moderní aspekty vědy: XLII. Díl mezinárodní kolektivní monografie. Česká republika: Mezinárodní Ekonomický Institut s.r.o., 2024, pp. 259—286. doi:10.52058/42-2024
[31]V. Yashchuk. Metodyka zabezpechennia bezpeky informatsiinykh system ta reahuvannia na kiberintsydenty kiberbezpekovymy tsentramy. Scientific Collection «InterConf+», vol. 45(201), Proceedings of the 8th Int. Sci. and Practical Conference, May 19—20, 2024, Brighton, UK, pp. 632—641. doi:10.51582/interconf.19-20.05.2024

[32]V. Yashchuk, Y. Demyanchuk, V. Savitska. Integrative approach to the analysis, modeling, and ensuring cyber security of critical information infrastructure under modern threats. Baltic Journal of Economic Studies, vol. 11, no. 2, 2025, pp. 273—286. doi:10.30525/2256-0742/2025-11-2-273-286

[33]J. Ruohonen. A look at the time delays in CVSS vulnerability scoring. Applied Computing and Informatics, vol. 15, no. 2, 2019, pp. 129—135. doi:10.1016/j.aci.2017.12.002

[34]M. Alkinoon, H. Althebeiti, A. Alkinoon, M. Mohaisen, S. Salem, D. Mohaisen. Industry-specific vulnerability assessment. In: M. Barhamgi, H. Wang, X. Wang (eds), Web Information Systems Engineering — WISE 2024, LNCS, vol. 15440, Springer, Singapore, 2025. doi:10.1007/978-981-96-0576-7_10

[35]A. Felkner et al. Vulnerability and attack repository for IoT: Addressing challenges and opportunities in Internet of Things vulnerability databases. Applied Sciences, vol. 14, no. 22, 2024, 10513. doi:10.3390/app142210513

[36]R. Croft, M. A. Babar, M. M. Kholoosi. Data quality for software vulnerability datasets. In: 2023 IEEE/ACM 45th Int. Conf. on Software Engineering (ICSE), IEEE, 2023, pp. 121—133.

[37]H. Kekül, B. Ergen, H. Arslan. Comparison and analysis of software vulnerability databases. International Journal of Engineering and Manufacturing, vol. 12, no. 4, 2022, pp. 1—15.

[38]C. Theisen, L. Williams. Better together: Comparing vulnerability prediction models. Information and Software Technology, vol. 119, 2020, 106204. doi:10.1016/j.infsof.2019.106204