GIS Odyssey Journal

2025 • Volume 5 • Number 2

https://doi.org/10.57599/gisoj. 2025.5.2.121

Piotr Górny[1]

METHODS FOR IDENTIFYING CYBER THREATS IN GIS SYSTEMS. COMPARATIVE ANALYSIS

Abstract: Geographic Information Systems (GIS) play a vital role in managing spatial data and supporting decision-making processes across a range of sectors. They are becoming an essential tool in many industries, including crisis management, urban planning, transport and environmental protection. However, the large volume and complexity of the data they handle render GIS systems increasingly vulnerable to cyber threats. Therefore, it is crucial that these systems are safeguarded using contemporary threat detection methods. This article presents various threat detection approaches for GIS systems, including network traffic analysis, intrusion detection systems (IDS), artificial intelligence, and system vulnerability analysis. The strengths, weaknesses, effectiveness and practical applicability of these methods are highlighted. The analysis indicates that a multi-layered approach combining various threat identification techniques is necessary to ensure comprehensive protection of GIS systems.

Keywords: cybersecurity, Geographic Information Systems (GIS), identifying cyber threats, threat detection methods

Received: 3 June2025; accepted: 12 August 2025

[1] Military University of Technology, Faculty of Cybernetics, Warsaw, Poland ORCID ID: https://orcid.org/0000-0003-3181-6320, email: piotr.gorny@wat.edu.pl

Introduction with analysis of the state of the problems

The rapid development of information technology and the increasing integration of GIS systems with global networks are giving rise to new cybersecurity challenges. Hacker attacks, unauthorised data modifications, information theft and system disruptions can have serious operational and strategic consequences. Therefore, identifying and neutralising cyber threats in GIS systems is essential for ensuring the integrity and reliability of these technologies. Threat detection methods in this context include traditional intrusion detection systems and modern techniques based on artificial intelligence and heuristic analysis. The effectiveness of these methods depends on various factors, including the type of threat, the system's structure and the protective mechanisms employed.

This article aims to present a comparative analysis of various cyber threat detection methods in GIS systems, including those based on network traffic analysis, intrusion detection systems (IDS), artificial intelligence, and system vulnerability analysis.

The most common threats include:

- distributed denial of service (DDoS) attacks, which lead to system overload;
- SQL injection and cross-site scripting (XSS) attacks, which can lead to unauthorised access to the GIS database;
- unauthorised changes to spatial databases;
- impersonating legitimate systems to obtain information (phishing);
- API security vulnerabilities that can lead to data leaks.

The following methods of detecting potential threats were compared:

1. System log analysis
2. Vulnerability scanning
3. Penetration testing
4. Intrusion detection systems (IDS/IPS)
5. Anomaly analysis using AI/ML
6. GIS data integrity monitoring
7. Network traffic analysis
8. Security audits

The strengths, weaknesses, effectiveness and practical applicability of these methods were identified. The results of the analysis indicate the need for a multi-level approach that combines various threat identification techniques to ensure the comprehensive protection of GIS systems.

Geographic Information Systems (GIS) are the foundation of modern spatial analysis, enabling the collection, processing and visualisation of geographic data in various sectors, including urban planning and crisis management. However, the rapid development of information technology means that these systems are increasingly becoming the target of cyberattacks, which can lead to data manipulation and disruption to their functioning, with potentially serious consequences for critical infrastructure. Therefore, identifying threats to GIS systems is crucial to ensuring their reliability and the security of spatial data. This is a complex task involving many challenges.

The most important ones are:

1. The growing number and complexity of threats: Malicious attacks are evolving and becoming increasingly sophisticated. Cybercriminals use techniques such as advanced malware and the exploitation of security vulnerabilities, as well as artificial intelligence technology, to carry out attacks.
2. The size and distributed structure of GIS data: GIS systems operate on huge spatial data sets that are often distributed across multiple servers, which makes it difficult to consistently monitor threats and respond quickly to incidents.
3. Difficulties in detecting zero-day attacks: Attacks on unknown security vulnerabilities, known as zero-day attacks, are particularly challenging to detect as there are no recorded signatures for these threats.
4. Lack of uniform security standards: GIS systems can use different platforms, programming languages, and architectures, which makes it challenging to implement consistent threat identification mechanisms at every level.
5. Threats related to the integration of IoT and cloud technologies: As GIS systems become more closely linked to IoT sensors and cloud solutions, they become more vulnerable to attacks involving the takeover of IoT devices and the manipulation of data in the cloud.
6. Incident response time: Detecting a threat is only the first step; it is crucial to take remedial action quickly. Delays in identifying and analysing cyber-attacks can lead to serious data loss or disruption to GIS systems.
7. Legal and regulatory aspects: Differences in data protection and cybersecurity regulations mean organisations must adapt their GIS systems to various national and international standards, often complicating the implementation of effective threat identification mechanisms.

This article aims to provide a comparative analysis of various methods for detecting cyber threats in GIS systems. It takes into account approaches based on network traffic analysis, intrusion detection systems (IDS), artificial intelligence, and system vulnerability analysis.

Material and methods

Effective identification of cyber threats requires the continuous improvement of analytical methods, the adaptation of new technologies and the cooperation of GIS and cybersecurity experts (Kirti Vasdev 2020). This has resulted in an increasing need for effective identification and protection against cyber threats.

The open nature of Geographic Information Systems (GIS), their integration with Internet of Things (IoT) systems and their real-time processing of large amounts of data make them particularly vulnerable to cyber threats. In 2024, the ENISA report identified seven major cybersecurity threats (ENISA 2024), see Figure 1.

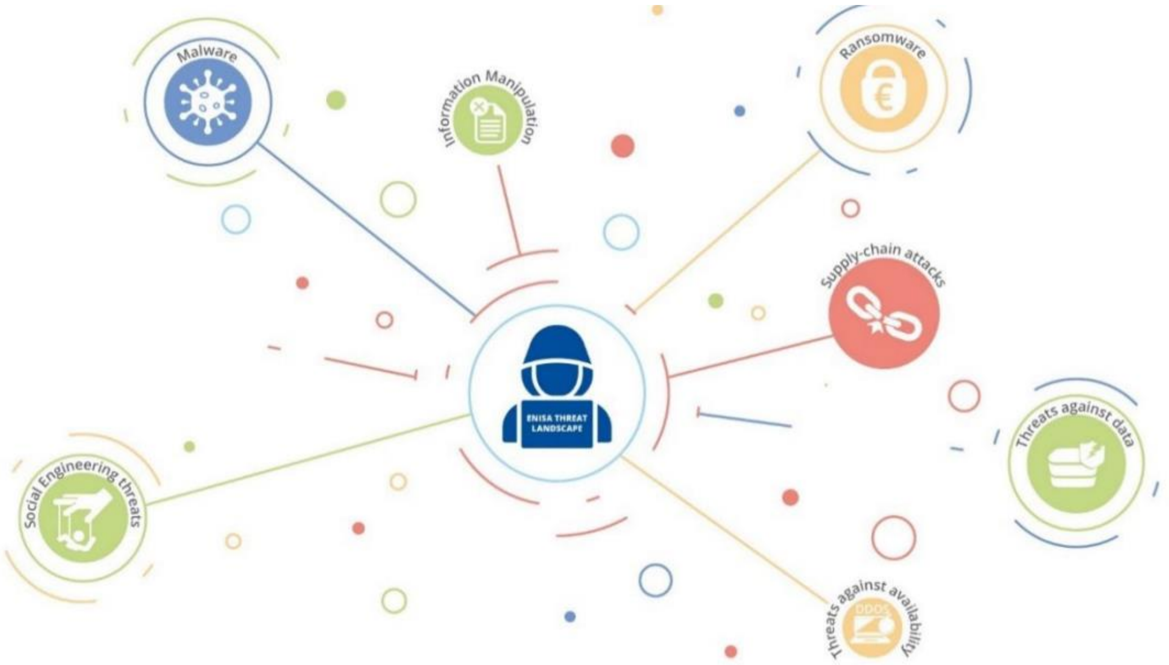

Figure 1. ENISA Threat Landscape 2024 – Prime threats
Source: ENISA Threat Landscape (2024)

The top threats are to availability, followed by ransomware and data threats. The report provides an in-depth analysis of each of these, based on an examination of several thousand publicly reported cyber security incidents and events.

The key findings of the ENISA Threat Landscape 2024 report are:

- The biggest threat: attacks on availability – cybercriminals are increasingly using Denial of Service (DoS) attacks to block access to key systems.
- Ransomware still at the top – attacks that encrypt data and demand a ransom remain one of the most serious threats to organisations.
- Threats to data – manipulation, theft and damage to spatial data are becoming increasingly common.
- The growing role of social engineering – cybercriminals use social engineering to deceive users and gain access to systems.
- Information manipulation – disinformation and falsification of geographic data can lead to poor decision-making in crisis management.
- Supply chain attacks – cyber threats arising from the vulnerability of GIS technology providers are becoming increasingly significant.

In connection with the NIS2 Directive (Network and Information Security Directive 2) coming into force in 2024, the ENISA 2024 report provides an analysis of cyber security threats in various sectors.

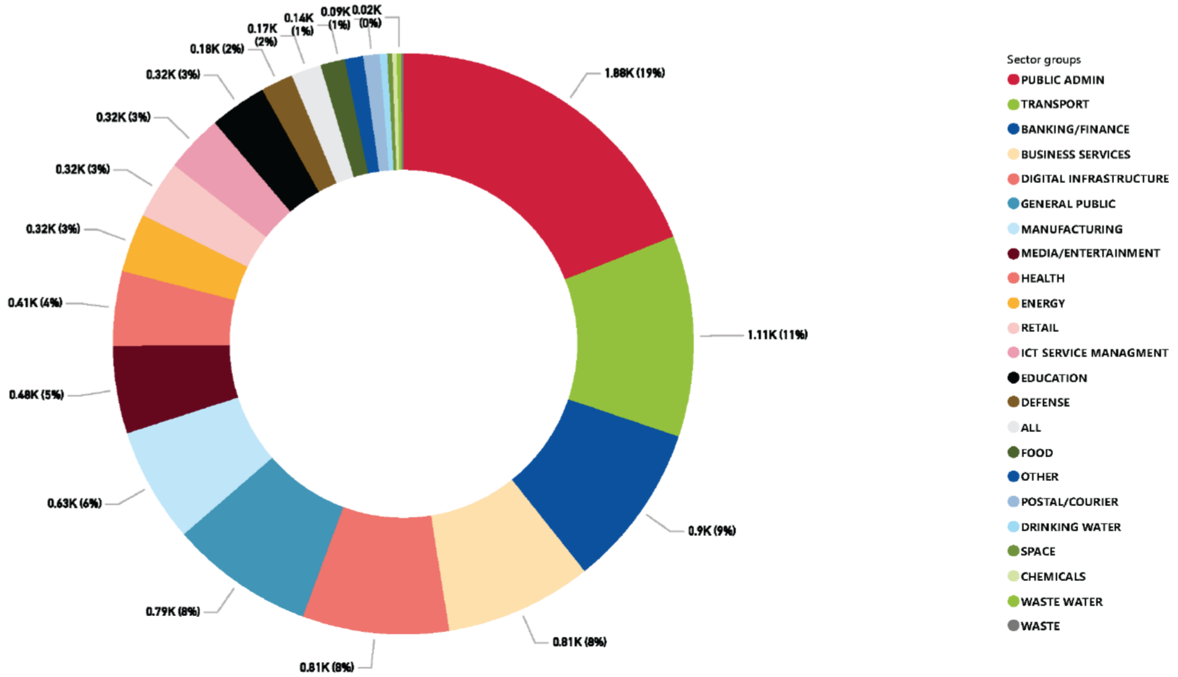

Figure 2. Targeted sectors per number of incidents, July 2023 – June 2024
Source: ENISA Threat Landscape (2024)

Notably, a significant proportion of incidents target organisations in the public administration (19%) and transport (11%), and finance (9%) sectors have been observed again (Figure 2). The report also highlights the increased activity of hacktivists and cybercriminals linked to states, which affects the stability of GIS systems and other critical infrastructure.

Results and discussion

This section of the article provides a general overview of selected methods for identifying cyber threats and compares their advantages and disadvantages.
The comparison of identification methods in the ENISA report includes various techniques and tools used to detect and respond to cyber threats. The analysis demonstrates how different methods impact the overall security posture of organizations and their critical infrastructure. Furthermore, it highlights the necessity of continuous improvement and adoption of advanced technologies to stay ahead of evolving cyber threats.

System log analysis. System logs play a key role in identifying and monitoring cyber threats to GIS systems. They provide a record of operational events, authentication, data access and anomalies in the operation of the IT infrastructure. Their effective analysis makes it possible to detect attacks, unauthorized access attempts, data manipulation and other disturbing activities in real time (Best practices for event logging and threat detection).

Key aspects of log analysis in GIS:

- Anomaly detection – analyze system access patterns and unusual user activities.
- Identifying unauthorized login attempts – recording erroneous authentication attempts that may indicate brute force attacks.
- Monitoring administrative activity – tracking changes in system configuration and modifications to user privileges.
- Event correlation – linking different logs to identify complex attacks, such as ransomware or phishing.
- Analysis automation – using SIEM (Security Information and Event Management) systems and artificial intelligence-based tools to quickly detect threats.
- Effective log analysis in GIS systems requires the application of advanced data analysis methods, filtering, and information visualization to enable quick responses to cyber threats (Awotipe, 2019).

Vulnerability scanning. Vulnerability Scanning plays a crucial role in identifying cyber threats in GIS systems. It allows for the detection of weak points in infrastructure and potential attack vectors. Vulnerability Scanning is the process of identifying weak points in GIS systems that can be exploited by cybercriminals. It involves automatically analyzing the infrastructure for known security vulnerabilities, allowing them to be quickly detected and eliminated. Its advantage is its effectiveness in identifying vulnerabilities and the ability to integrate with security management systems. However, scanning also has limitations – it can generate false alarms and may not detect new, unknown threats (Turner & Malik, 2021).

The process of vulnerability scanning consists of several key stages that enable the effective detection of security vulnerabilities in GIS systems. Here are the main steps (OpenSecurity.pl):

- Information gathering – identifying active devices, services, and applications in the GIS system to determine potential areas of threats.
- Selection of scanning method – deciding whether the scan will be performed locally, remotely, or using SIEM tools.
- Conducting the scan – using dedicated tools to identify known vulnerabilities, such as scanners like OpenVAS, Nessus, or Qualys.
- Result analysis – interpreting data collected during the scan, classifying detected vulnerabilities according to risk level.
- Reporting – preparing a report with scan results, indicating priority threats and recommendations for their elimination.
- Implementing countermeasures – applying patches, configuring security settings, updating software to remove vulnerabilities.
- Rescanning – conducting control tests to verify the effectiveness of implemented security measures and ensuring the vulnerability has been eliminated.

Penetration testing. Penetration Testing is a method of assessing the security of GIS systems by simulating real cyberattacks. Its goal is to identify weak points in the infrastructure that can be exploited by cybercriminals.

Conducted by ethical hackers, these tests allow for the detection of vulnerabilities in applications, databases, networks, and system configurations. Thanks to penetration tests, organizations can better prepare for potential threats and implement effective protection mechanisms. The main stages of penetration testing include information gathering, vulnerability analysis, system exploration, result reporting, and the implementation of security measures.

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) play a crucial role in identifying cyber threats in GIS systems.

IDS monitors network traffic and system logs to detect suspicious activities that may indicate unauthorized access attempts or attacks. IDS does not take preventive actions – it only alerts administrators of potential threats.

IPS operates proactively – it not only detects intruders but also automatically blocks their actions, such as rejecting malicious data packets or blocking specific IP addresses. Both systems can be integrated with GIS solutions, providing an additional layer of protection against DDoS attacks, system exploits, and unauthorized access (25 Best Intrusion Detection, 2025).

In the Table 1 is a comparison of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) in the context of identifying cyber threats in GIS systems.

Table 1. Comparison of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)

Feature	IDS (Intrusion Detection System)	IPS (Intrusion Prevention System)
Main Function	Detects and records suspicious activities in the network or system.	Detects threats and automatically blocks potential malicious actions.
Response to Threat	Alerts administrators to a potential attack but does not take preventive actions.	Blocks or neutralizes the threat in real-time.
Application in GIS	Helps monitor unauthorized access attempts to GIS systems and databases.	Protects GIS systems from exploits, malware, and DDoS attacks.
Impact on Performance	Does not directly affect the system's operation as it only monitors traffic.	May cause network delays due to the need to analyze and block traffic.
Detection Accuracy	May generate false alarms, requiring analysis by an administrator.	May block legitimate network traffic if rules are improperly configured.
Implementation Cost	Generally lower than IPS as it does not require advanced defensive mechanisms.	Higher cost due to threat blocking functions and the need for frequent updates.

Source: own study

In summary, IDS is effective for monitoring and threat analysis, whereas IPS provides active protection by eliminating unwanted actions. Depending on the level of security required in GIS systems, organizations often use both solutions simultaneously (Chęciński).

Here are some IDS/IPS tools used in GIS systems (25 Best Intrusion Detection, 2025):

- Snort – a popular open-source IDS that analyzes network traffic and detects suspicious activities based on threat signatures.

- Suricata – an advanced IDS/IPS system that supports multi-threaded data processing and integration with SIEM systems.
- Zeek (formerly Bro) – an IDS tool focused on network traffic analysis, often used in cybersecurity research.
- Cisco Firepower – a commercial IPS that offers advanced threat detection and blocking features in real-time.
- Palo Alto Networks IDS/IPS – a solution integrated with next-generation firewalls, providing protection against exploits and network attacks.

Each of these tools has its unique features and can be tailored to the specific needs of GIS systems.

Anomaly analysis using artificial intelligence (AI) and machine learning (ML). Anomaly analysis using artificial intelligence (AI) and machine learning (ML) is a modern approach to identifying cyber threats in GIS systems. ML techniques allow for the detection of unusual patterns in user activity, network traffic, and system operations that may indicate intrusion attempts, malware attacks, or unauthorized access (Machine Learnin, 2025).

The main advantages of this approach are the ability to automatically process large data sets, detect threats in real time, and adapt to new types of attacks. Popular methods used in anomaly analysis include supervised and unsupervised models such as neural networks, classification algorithms, and outlier detection.

Here are some AI/ML algorithms used in anomaly analysis in GIS systems:

- Machine Learning (ML) – Uses classification and regression models to identify unusual patterns in GIS data.
- Neural Networks (NN) – Used for analyzing large data sets, enabling the detection of subtle anomalies in real time.
- User and Entity Behavior Analytics (UEBA) – Monitors user activity and detects deviations from typical behavior, which may indicate intrusion attempts.
- Time Series Analysis – Identifies anomalies in GIS data based on changes over time, e.g., sudden increases in network traffic.

In summary, anomaly analysis using AI/ML is a powerful tool in detecting cyber threats in GIS systems, but its effectiveness depends on the quality of data and proper implementation.

Monitoring the integrity of GIS data. Monitoring the integrity of GIS data is a key process in identifying cyber threats, ensuring the accuracy, consistency, and security of stored information. It involves detecting unauthorized changes, tampering, or damage to spatial data that may result from cyber-attacks, system errors, or hardware failures.

It utilizes technologies such as checksum controls, audit systems, blockchain mechanisms, and AI/ML algorithms to detect anomalies in the structure of GIS data. Upon detecting violations, administrators can implement recovery procedures, analyze the source of threats, and improve security mechanisms (Morozov, 2024).

Here are some tools used for monitoring the integrity of GIS data:

- ArcGIS Pro – offers a set of tools for managing spatial data, including integrity and data editing control mechanisms.

- QGIS – free GIS software that enables spatial data analysis and validation in terms of consistency and correctness.
- PostGIS – an extension for PostgreSQL that supports geo-spatial data analysis and provides data integrity control mechanisms.
- Blockchain for GIS – blockchain technology can be used to secure and track changes in GIS data, ensuring their immutability and authenticity.
- Geopandas – a Python library for spatial data analysis, allowing for the detection of anomalies and discrepancies in GIS datasets.

Monitoring the integrity of GIS data is a crucial aspect of cybersecurity, but its effectiveness depends on proper implementation and adaptation to the organization's needs.

Implementation complexity – requires advanced control mechanisms and adjustments to specific GIS requirements.

Protection against tampering – safeguards against deliberate falsification of GIS data, e.g., by cybercriminals. High resource demand – monitoring systems can strain IT infrastructure and require high computational power.

Integration with security systems – can work with IDS/IPS, SIEM, and blockchain, enhancing protection. Cost of implementation and maintenance – developing effective monitoring requires investment in hardware and software.

Error detection – allows for quick identification and repair of technical issues. Possibility of false alarms – some changes may be wrongly classified as threats.

Increased trust in data – enables verification of the correctness of information used in GIS systems. Need for continuous update of mechanisms – new methods of attacks require regular improvement of the system.

Monitoring the integrity of GIS data is a crucial aspect of cybersecurity, but its effectiveness depends on proper implementation and adaptation to the organization's needs.

Network Traffic Analysis (NTA). Network Traffic Analysis (NTA) is a method of monitoring and evaluating data traffic in a network to identify potential cyber threats in GIS systems. It allows detecting anomalies, suspicious transmissions, and unauthorized access attempts that may indicate DDoS attacks, malware, or data exfiltration.

NTA techniques involve packet monitoring, identifying unusual traffic patterns, analyzing network protocols, and using AI/ML tools to detect threats in real-time. This enables organizations to respond more quickly to security incidents and better protect their GIS resources.

Tools used for network traffic analysis in GIS systems include:

- Wireshark – an advanced packet analyzer that captures and analyzes network traffic in real-time.
- tcpdump – a command-line packet capture tool often used in Linux and Unix environments.
- Snort – an intrusion detection system (IDS) that analyzes network traffic for suspicious activities.

- ntopng – a tool for visualizing and analyzing network traffic, which helps identify anomalies and optimize network performance.
- ArcGIS Network Analyst – a GIS tool for analyzing transport networks that can be used to monitor traffic in GIS systems.

Network traffic analysis is an essential cybersecurity tool in GIS systems, but its effectiveness depends on proper implementation and adaptation to specific needs (5 Types of Network Analysis in GIS, 2025).

Security audits. Security audits are a key process in identifying cyber threats in GIS systems. They involve a comprehensive analysis of the infrastructure, procedures, and protection mechanisms to detect potential weaknesses and vulnerabilities to attacks.

Audits may include system configuration analysis, access policy review, penetration tests, log system analysis, and compliance assessment. Their aim is to increase the level of security, eliminate gaps, and recommend corrective actions (Palatty, 2024).

Here are some tools used in GIS system security audits:

- Globema GIS Security Audit – a comprehensive analysis of GIS system security, covering hardware, network infrastructure, and software components.
- Esri Security Operations – GIS tools supporting incident and risk management, integrating real-time data.
- ISO 27001 Security Audit – standards related to information security management, applied in GIS system audits.

Security audits are a crucial tool in protecting GIS systems, but their effectiveness depends on the thoroughness of execution and regular reviews.

Summary of the advantages and disadvantages of cyber threat identification methods is included in Table 2.

Table 2. Summary of the advantages and disadvantages of cyber threat identification methods

Identification methods	**Advantages**	**Disadvantages**
System log analysis	Early threat detection – logs allow identifying anomalies indicating attempted intrusions or other attacks.	Large amount of data – log analysis can be time-consuming and require significant computational resources.
	Tracking user activity – logs record actions in the system, which helps in audits and detecting unauthorized operations.	Need for specialized knowledge – interpreting logs requires advanced cybersecurity knowledge.
	Automation of analysis – AI tools can help detect patterns indicating threats.	Risk of false alarms – not all detected anomalies indicate actual threats, which can lead to erroneous decisions.
	Compilation of evidence – logs can be used as evidence in security incident analyses.	Problem with log integrity – if logs are not properly secured, they can be manipulated by an attacker.
	Integration with SIEM systems – Security Information and Event Management systems assist in effective log analysis.	Costs – implementing effective log analysis mechanisms can be expensive.

Identification methods	**Advantages**	**Disadvantages**
Vulnerability Scanning	Early threat identification – scanning helps detect security vulnerabilities before they are exploited by cybercriminals.	Risk of false positives – scanners can generate both false alarms and miss certain vulnerabilities.
	Automation of the process – scanning tools can operate continuously and detect vulnerabilities without human intervention.	Possible system disruptions – intensive scanning may burden the network or system resources.
	Integration with security management systems – scanning results can be used in SIEM systems for better threat analysis.	Does not detect all threats – scanners focus on known vulnerabilities but may not detect new or more complex attacks.
	Support for regulatory compliance – organizations can use vulnerability scanning to meet legal and certification requirements.	Need for regular updates – vulnerability databases must be frequently updated to account for new threats.
	Reduction in response time to threats – quick detection of vulnerabilities enables faster implementation of countermeasures.	Implementation cost – advanced scanning tools may require financial and technical investments.
Penetration Testing	Realistic attack simulation – tests replicate the actual methods used by cybercriminals.	Time-consuming – requires careful planning and execution, which can take a lot of time.
	Identification of real vulnerabilities – detects actual weaknesses that can be exploited in an attack.	Cost – professional penetration tests can be expensive, especially for large organizations.
	Security level assessment – allows for a comprehensive analysis of the effectiveness of existing protection mechanisms.	Risk of system disruption – tests can cause service interruptions or slowdowns.
	Increased security awareness – enhances the IT team's knowledge about threats and defense methods.	Requires advanced knowledge – conducting tests requires specialized cybersecurity skills.
	Regulatory compliance – helps in aligning the GIS system with data protection standards and regulations.	Limited scope – tests may not cover all possible attack vectors, especially new and advanced techniques.
Anomaly analysis using artificial intelligence (AI) and machine learning (ML)	Detection of unknown threats – AI/ML can identify new and unusual threats that traditional security systems might miss.	Complexity of implementation – requires significant computational resources and specialized knowledge for effective deployment.
	Automation of analysis – reduces the need for manual log analysis, saving administrators' time.	Risk of false alarms – ML models can generate incorrect alerts if not properly calibrated.
	Adaptability to new attacks – systems learn continuously, allowing for dynamic adjustment to changing methods of cybercriminals.	Requirement for large amounts of data – effectiveness depends on the quality and quantity of training data, which can be time-consuming to collect.
	Integration with other security systems – AI/ML analyses can work with IDS/IPS and SIEM, enhancing protection efficiency.	Costs of deployment and maintenance – developing and maintaining such systems involves investments in hardware and software.
	Capability of behavioral analysis – AI/ML can identify unauthorized user activity by analyzing typical behavior patterns.	Need for continuous model updates – algorithms require regular improvement to keep up with new threats.

Identification methods	Advantages	Disadvantages
Monitoring	Ensuring data consistency – monitoring allows for the detection of unauthorized changes or data damage.	Implementation complexity – requires advanced control mechanisms and adjustments to specific GIS requirements.
	Protection against tampering – safeguards against deliberate falsification of GIS data, e.g., by cybercriminals.	High resource demand – monitoring systems can strain IT infrastructure and require high computational power.
	Integration with security systems – can work with IDS/IPS, SIEM, and blockchain, enhancing protection.	Cost of implementation and maintenance – developing effective monitoring requires investment in hardware and software.
	Error detection – allows for quick identification and repair of technical issues.	Possibility of false alarms – some changes may be wrongly classified as threats.
	Increased trust in data – enables verification of the correctness of information used in GIS systems.	Need for continuous update of mechanisms – new methods of attacks require regular improvement of the system.
Network Traffic Analysis	Early threat detection – allows identifying anomalies in network traffic that indicate possible attacks.	Resource-intensive – network traffic analysis can be burdensome for the system.
	Real-time monitoring – enables immediate response to suspicious activities.	Risk of false positives – some atypical patterns may be incorrectly interpreted as threats.
	Integration with other security systems – can work with IDS/IPS and SIEM, enhancing security effectiveness.	Complexity of implementation – requires specialized knowledge and appropriate adaptation to the GIS infrastructure.
	Identification of unauthorized activities – helps detect intrusion attempts, data exfiltration, and other cyberattacks.	Implementation cost – advanced solutions may require significant financial investment.
	Improved network management – analysis helps optimize network traffic and identify performance issues.	Requires continuous updates – attacks evolve, so analysis tools must be regularly adjusted.
Security audits	Comprehensive security assessment – audits allow for a thorough analysis of GIS systems, identifying weaknesses and recommending corrective actions.	Time-consuming – conducting a full audit requires a detailed review of the infrastructure, which can be time-intensive.
	Compliance with regulatory requirements – helps in aligning the GIS system with security standards, such as ISO 27001 or NIST.	Implementation cost – professional audits can be expensive, especially in large organizations.
	Identification of unknown vulnerabilities – audits can detect threats that have not been identified by other security mechanisms.	Risk of superficial analysis – if the audit is not conducted thoroughly, it may not cover all attack vectors.
	Improved security awareness – increases the knowledge of GIS administrators and users about threats and best protection practices.	Need for regular audits – a single audit does not provide long-term protection; periodic system reviews are required.
	Integration with other tools – audit results can be used to optimize IDS/IPS systems, SIEM, and network traffic analysis.	Need for specialized knowledge – effective analysis requires experts in cybersecurity and GIS.

Source: own study

Conclusions

In this article, the author attempts to evaluate selected methods. As shown, each method for identifying cyber threats in GIS systems has its advantages and disadvantages. A general summary of each method is provided below.

Log analysis involves reviewing and interpreting event records logged by information systems. This allows for the identification of irregularities and suspicious activities that may indicate potential security threats.

Vulnerability scanning is an automated process of scanning information systems to detect weak points that can be exploited by cybercriminals. This enables quick identification and remediation of vulnerabilities.

Penetration testing, also known as pentests, are simulated attacks conducted by security specialists to identify vulnerabilities in GIS systems. They allow for assessing the effectiveness of existing security mechanisms and implementing additional protective measures.

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) monitor network traffic in real-time, analyzing it for suspicious activities. IDS informs administrators of detected potential threats, whereas IPS can automatically block suspicious activities.

Anomaly analysis using artificial intelligence (AI) and machine learning (ML) involves employing algorithms that learn normal behavioral patterns of GIS systems to subsequently detect deviations from these patterns. This allows for the identification of previously unknown threats.

GIS data integrity monitoring includes regularly checking the consistency and accuracy of data stored in GIS systems. This enables the detection of unauthorized changes and potential data security breaches.

Network traffic analysis involves monitoring and interpreting data transmitted over the network in real-time. This allows for the detection of unauthorized activities and identifying patterns that may indicate cyber-attacks.

Security audits are comprehensive reviews of GIS systems conducted by specialists to assess compliance with security standards, identify vulnerabilities, and recommend remedial measures. These audits are crucial for ensuring the long-term protection of systems.

Each of these methods has its own unique advantages and limitations, and an effective strategy for protecting GIS systems often requires their integrated application. Proper protection of GIS systems requires a holistic approach and regular monitoring of their security status.

Acknowledgements

This work was financed/co-financed by Military University of Technology under research project UGB 531-000023-W500-22.

References

25 Best Intrusion Detection & Prevention Systems (IDS &IPS) in 2025. https://cybersecuritynews.com/intrusion-detection-prevention-systems/ [access: 15.04.2025].

5 Types of Network Analysis in GIS. https://gisgeography.com/network-analysis/ [accessed: 12.04.2025].

Awotipe O. (2019). Log Analysis Key to Cyber Threat Detection, Iowa State University.

Best practices for event logging and threat detection. https://www.cyber.gov.au/sites/default/files/2025-03/Best%20practices%20for%20event%20logging%20and%20threat%20detection%20%28August%202024%29.pdf [access: 11.04.2025].

Chęciński W. Kompendium wiedzy – IDS i IPS (*Compendium of knowledge – IDS and IPS*). https://whitehats.pwr.edu.pl/research/kompendium-ids-ips/ [access: 14.04.2025].

ENISA Threat Landscape (2024). September 2024. European Union Agency for Cybersecurity (ENISA). https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 [access: 15.04.2025].

Machine Learning for Anomaly Detection (2025). https://www.geeksforgeeks.org/machine-learning-for-anomaly-detection/ [access: 10.04.2025].

Morozov V. (2024). Data Integrity Testing: Techniques, Tools, and Best Practices. https://luxequality.com/blog/data-integrity-testing/ [access: 15.04.2025].

Network and Information Security Directive 2 (NIS2). https://www.nis2-info.eu/full-text/ [access: 15.04.2025].

Palatty N.J. (2024). 7 Best Security Audit Tools: A Complete Guide. https://www.getastra.com/blog/security-audit/security-audit-tools/ [access: 23.03.2025].

Systemy wykrywania i zapobiegania włamaniom (IDS/IPS) *(Intrusion detection and prevention systems-IDS/IPS).* https://ccit.pl/systemy-wykrywania-i-zapobiegania-wlamaniom-ids-ips/ [access: 15.04.2025].

Turner H., Malik S. (2021). System Vulnerability Assessment in Geospatial Networks. Computer Security Journal, 33(2), 11–29.

Vasdev K. (2020). GIS in cybersecurity: mapping threats and vulnerabilities with geospatial analytics. International Journal of Core Engineering & Management, vol. 6, no. 8.