

The Strategic Role of Monitoring in Modern Critical Infrastructure Management

Ferenc Bálint

University of Óbuda, Hungary

ORCID ID:

0009-0009-8970-762X

ABSTRACT

In today's interconnected world, effective infrastructure monitoring tools are essential for maintaining the performance, security, and reliability of IT systems. Advanced monitoring techniques have played a key role in enhancing IT security and operational efficiency, especially as infrastructures grow more complex and cyber threats intensify. This article explores the evolution of monitoring solutions, from traditional methods to today's sophisticated, AI-powered tools. Core IT monitoring technologies - such as Security Information and Event Management (SIEM), Security Information Monitoring (SIM), Application Performance Management (APM), and system and network monitoring - form a comprehensive framework for overseeing both security and performance. These tools have evolved to detect threats, automate responses, and maintain system reliability across industries. Recent advancements include the integration of automation, Artificial Intelligence (AI), and Machine Learning (ML), enabling predictive threat detection, anomaly recognition, and automated mitigation. These AI-driven capabilities improve efficiency, reduce false positives, and strengthen the overall security and performance of critical systems. With the increasing demands of real-time data analysis and rapidly evolving cyber threats, integrated monitoring solutions are vital for proactive risk management. By combining SIEM, SIM, APM, and AI technologies, organizations can enhance their security posture and ensure the resilience of critical infrastructure in a dynamic digital environment.

General Terms

Infrastructure Monitoring: Tools and techniques essential for maintaining the performance, security, and reliability of IT systems.

Keywords

AI, application, cloud, infrastructure, cybersecurity, tool, monitoring, performance

1. INTRODUCTION

Critical infrastructures are essential to the functioning of modern society, supporting vital services such as electricity, water supply, transportation, communication, healthcare, and financial systems. These systems are increasingly exposed to cyberattacks, natural disasters, and technical failures, which can result in widespread economic and social disruption. Protecting their security and ensuring uninterrupted operations is a top priority.

Major threats originate from cybercriminals, terrorist groups, and state-sponsored actors attempting to disrupt or damage critical services. Natural hazards like floods, earthquakes, and severe weather also pose serious risks. Additionally, human errors and equipment failures can lead to major breakdowns if

not properly managed. Safeguarding measures include cybersecurity defenses, emergency planning, structural reinforcements, and routine inspections.

In a highly connected world, continuous 24/7 monitoring is vital to detect and respond to issues before they escalate. AI-driven monitoring tools offer real-time alerts, anomaly detection, and automated responses, helping organizations stay ahead of threats while optimizing performance.

Monitoring must cover all layers of IT infrastructure, from networks and applications to databases and storage systems. Tools such as Application Performance Management (APM) provide visibility into application behavior, detect slowdowns, and enable dynamic scaling during peak usage, such as sales events or service outages.

As infrastructure environments grow more complex and distributed, monitoring must also account for mobile apps, web platforms, cloud services, and security features like biometrics or PINs. AI and automation are critical in simplifying oversight, reducing manual workloads, and improving overall system resilience.

By implementing advanced monitoring solutions, organizations can better manage risks, maintain operational continuity, and ensure that critical infrastructure services remain reliable and secure - even in the face of evolving challenges. [1].

2. EVOLUTION AND LANDSCAPE OF INFRASTRUCTURE MONITORING AND AUTOMATION

Infrastructure monitoring has evolved significantly, shifting from manual oversight to intelligent, automated systems. In its early days, monitoring relied on reactive responses and basic tools that offered limited visibility. The introduction of automation enabled proactive management, reducing downtime and improving operational efficiency.

The incorporation of artificial intelligence further advanced monitoring practices. AI-powered tools can now analyze data patterns, predict failures, and adapt to changing environments in real time. These capabilities have made IT infrastructure more agile, responsive, and resilient.

Industry-specific requirements have played a major role in shaping monitoring solutions. Sectors like healthcare require real-time oversight of life-critical systems, while the financial industry focuses on secure, reliable monitoring of high-volume data transactions. These demands accelerated the development of specialized tools to ensure both performance and protection.

As cloud adoption surged, organizations increasingly turned to cloud-native monitoring tools capable of managing

dynamic and distributed workloads. Tools that support continuous monitoring, automation, and rapid incident response have become essential in today's digital-first landscape.

Effective monitoring is a cornerstone of any IT environment. In particular, Security Information Monitoring (SIM) has become a critical component for defending infrastructure against evolving cyber threats. SIM tools integrate with IT systems to deliver real-time visibility, threat detection, and response capabilities. Leading platforms, such as Microsoft Azure Sentinel, provide advanced analytics and automated workflows for identifying and mitigating threats quickly. Alongside Azure Sentinel, other robust SIM tools continue to emerge, offering organizations various options tailored to their unique environments and risk profiles.

Market leaders like Microsoft, IBM, and Cisco have long influenced infrastructure monitoring with comprehensive platforms. Microsoft's System Center suite, for example, remains a foundational solution for managing and automating IT operations. Simultaneously, modern innovators like Datadog, Splunk, and Dynatrace have introduced highly adaptive, cloud-centric monitoring platforms.

Collaboration across the industry continues to drive innovation. Partnerships between software vendors, hardware manufacturers, and cloud providers lead to integrated, scalable solutions that meet the complex needs of modern enterprises. Understanding both the legacy and emerging players in this space helps organizations make informed, strategic decisions about their monitoring and automation investments. [2].

3. ADDRESSING CYBERSECURITY RISKS WITH SIEM SOLUTIONS

In today's digital landscape, cybersecurity risks have escalated dramatically, particularly for industrial control systems (ICS). The convergence of information technology (IT) and operational technology (OT) has created complex environments where cyber threats can have real-world consequences, including disruption of essential services and compromise of critical infrastructure. These environments have become prime targets for nation-state actors and sophisticated cybercriminal groups who are increasingly using advanced tactics to breach defenses and evade detection. The range of threats continues to expand, encompassing ransomware that halts operations, phishing schemes aimed at high-level executives, social engineering tactics that manipulate personnel, and malware capable of crippling utility systems.

To defend against such sophisticated and persistent threats, organizations are increasingly relying on Security Information and Event Management (SIEM) systems as central components of their cybersecurity strategies. SIEM solutions provide real-time collection, correlation, and analysis of security data from across an organization's network. By aggregating logs and event information from a multitude of sources - including firewalls, intrusion detection systems, endpoint protection tools, and servers - SIEMs generate a comprehensive view of an organization's security posture. This unified perspective allows security teams to detect anomalies and identify emerging threats before they escalate into full-scale incidents. Figure 1.

Functionality	ArcSight	QRadar	McAfee	LogRhythm	USM-CSSIM	ISA	Splunk	SolarWinds
Correlation rules	•	•	•	•	•	•	•	•
Data sources	•	•	•	•	•	•	•	•
Real time processing	•	•	•	•	•	•	•	•
Data volume	•	•	•	•	•	•	•	•
Visualization	•	•	•	•	•	•	•	•
Data analytics	•	•	•	•	•	•	•	•
Performance	•	•	•	•	•	•	•	•
Forensics	•	•	•	•	•	•	•	•
Complexity	•	•	•	•	•	•	•	•
Scalability	•	•	•	•	•	•	•	•
Risk analysis	•	•	•	•	•	•	•	•
Storage	•	•	•	•	•	•	•	•
Price	•	•	•	•	•	•	•	•
Resilience	•	•	•	•	•	•	•	•
Reaction and reporting	•	•	•	•	•	•	•	•
UEBA	•	•	•	•	•	•	•	•
Security	•	•	•	•	•	•	•	•

— Low/Basic • Average • High/Advanced.

Figure 1: Analysis of different SIEM solutions [8]

One of the core strengths of SIEM systems is their ability to correlate events that, in isolation, might seem benign but collectively indicate malicious activity. These correlations are driven by rule-based engines or, increasingly, by more dynamic machine learning models capable of identifying complex patterns of behavior. As a result, SIEM platforms have evolved from simple log collectors into intelligent systems that assist analysts in uncovering hard-to-detect threats, including insider threats and low-and-slow attacks that unfold over extended periods.

The modern SIEM is not only about detection but also about enabling fast and informed responses. Real-time alerting and customizable dashboards allow security teams to prioritize incidents and respond with speed and precision. Many SIEMs also integrate with automated response systems, enabling certain threats to be mitigated immediately - though the depth and effectiveness of automation vary significantly across different platforms. Some systems merely trigger alerts, while others can quarantine devices, block IP addresses, or invoke playbooks for incident response, often guided by pre-configured risk thresholds.

Data visualization plays a pivotal role in SIEM functionality. Without clear and intuitive visual representations, the value of collected data can be lost in complexity. Advanced SIEMs provide interactive dashboards and graphical summaries that make it easier for analysts to identify patterns, track security trends, and understand incidents in context. This enhanced visibility not only aids in incident response but also supports forensic investigations, compliance reporting, and executive-level briefings.

Equally important is the system's scalability and performance. As organizations grow, so does the volume of data being generated, and SIEM solutions must be able to scale accordingly. High-performance SIEMs are built to handle millions of events per second without compromising on speed or accuracy. Efficient indexing, data normalization, and storage architectures are essential to ensure that systems remain responsive even under significant load. Yet, due to storage limitations and cost, many SIEM platforms retain full event data for a limited time - commonly around 90 days - which presents a trade-off between long-term analysis and system performance.

Cost and deployment complexity remain important considerations when selecting a SIEM. Enterprise-grade solutions from vendors such as IBM, Microsoft (via Azure Sentinel), and Splunk offer powerful features but can require substantial investment in both financial and human resources. Meanwhile, other solutions like LogRhythm and AlienVault provide more accessible options that still deliver core

functionality, making them suitable for mid-sized organizations. Open-source alternatives offer potential cost savings but may lack advanced capabilities and require in-house expertise for setup and ongoing maintenance.

Organizations must also consider resilience and fault tolerance when choosing a SIEM. Since these systems sit at the heart of a security operations center, any interruption in monitoring can leave an organization vulnerable. Robust architectures that support high availability, failover capabilities, and disaster recovery are critical, especially for sectors with continuous uptime requirements like energy, healthcare, and finance.

The integration of behavioral analytics and risk assessment tools is further elevating the role of SIEMs. By assessing user and system behavior against known baselines, these platforms can flag activities that deviate from the norm - whether it's a user accessing files outside regular hours or a device making suspicious outbound connections. When combined with risk scoring features, SIEMs can help security teams focus their efforts on the most pressing vulnerabilities, improving both efficiency and effectiveness in threat management.

As cyber threats become more dynamic and multifaceted, the need for intelligent, adaptive, and robust SIEM systems becomes increasingly apparent. While the market offers a wide spectrum of solutions - from streamlined platforms for smaller enterprises to sophisticated, AI-driven ecosystems for large organizations - the underlying goal remains consistent: to provide visibility, enhance threat detection, and support a proactive security posture. The continued evolution of SIEM technology is essential for keeping pace with the constantly shifting cyber threat landscape, ensuring that organizations can defend themselves not just reactively, but with strategic foresight. [5]

4. SIEM'S INNOVATION IN BEHAVIOR ANALYTICS, VISUALIZATION AND STORAGE

Modern SIEM systems are increasingly expected to go beyond basic log collection and correlation by incorporating advanced behavioral and risk analysis functionalities. To meet these demands, organizations must develop sophisticated tools and methodologies that support the optimal deployment of diverse security mechanisms. This includes adopting multi-level, risk-based metrics that can guide adaptive responses within managed infrastructures. A comprehensive deployment framework should also include redundancy strategies and diverse sensor arrays to ensure broad, resilient coverage. These mechanisms not only enhance detection accuracy but also ensure that threat intelligence remains robust against complex, evolving attack vectors.

Despite the maturity of user-friendly graphical interfaces across most commercial SIEM solutions, significant limitations remain in how these systems handle the vast volume of data generated across complex environments. Visualization tools, while improving, often lack the depth and scalability needed to provide actionable situational awareness in real time. To address this, future enhancements must focus on advanced visualization and analysis modules capable of condensing large datasets into intuitive, strategic insights. This will empower security teams with improved decision-making and faster, more precise reaction capabilities.

Data storage continues to be a critical concern, both in terms of technical capacity and financial impact. While many SIEM

platforms offer robust storage features, they are frequently constrained by on-premise hardware limits and high licensing costs tied to data volume. These constraints make scalability a challenge, especially for long-term data retention and forensic investigations. In response, secure and elastic storage models leveraging "cloud-of-clouds" architectures have emerged as viable solutions. By distributing SIEM data across multiple public cloud providers - such as Amazon S3, Amazon Glacier, Microsoft Azure, or Google Cloud - organizations can achieve both resilience and customization. These architectures support tailored retention policies and offer cost-efficiency, aligning storage capabilities with compliance and operational needs.

Looking toward the future, the role of SIEM systems is poised to expand across multiple sectors, influenced by a confluence of political, economic, social, technological, environmental, and legal factors. In critical infrastructure sectors such as energy, healthcare, and transportation, SIEMs will remain foundational to cyber resilience. Their utility is also growing among small and medium enterprises (SMEs), many of which operate with limited in-house cybersecurity expertise. For these organizations, SIEM systems - especially cloud-based or managed variants - offer a scalable path to achieving visibility, compliance, and threat detection capabilities previously reserved for larger enterprises.

In conclusion, the evolution of SIEM technology reflects its critical function in securing modern digital ecosystems. With continued investment in behavioral analytics, sensor deployment frameworks, scalable storage solutions, and intelligent visualization tools, SIEMs are well-positioned to serve as central pillars of cybersecurity management across both large and small organizations.[5]

5. CHALLENGES IN INFRA-STRUCTURE MONITORING AND AUTOMATION ACROSS INDUSTRIES

In the world of infrastructure monitoring and automation, industries face a range of unique challenges that impact how they monitor and secure their operations. One of the most significant hurdles is regulatory compliance, which stands as a major concern for organizations across various sectors. Regulatory frameworks impose strict standards that IT operations must meet and ensuring monitoring and automation processes align with these standards is vital. For example, in healthcare, regulations like the Health Insurance Portability and Accountability Act (HIPAA) require healthcare organizations to maintain robust monitoring systems that safeguard patient data, ensuring its confidentiality, integrity, and availability. Achieving compliance in such environments necessitates real-time monitoring and automated responses to any breaches or vulnerabilities, underscoring the importance of expanding enterprise application monitoring while staying within regulatory boundaries.

Alongside regulatory compliance, the handling of sensitive data presents a significant challenge, especially in industries where information security is paramount. The financial sector, for instance, processes vast amounts of sensitive financial data, demanding sophisticated monitoring solutions that offer detailed insights without compromising the security of that information. This balancing act is crucial, as any compromise could lead to severe consequences. Understanding how industries address the balance between safeguarding sensitive data and maintaining effective monitoring systems is key to crafting efficient solutions.

Scalability is another challenge that industries facing rapid growth must confront. E-commerce and online services are prime examples, where monitoring systems must be able to scale horizontally to support growing user bases and increasing transaction volumes. Automation becomes an essential tool in these environments, helping to provision resources automatically, optimize performance, and ensure that the monitoring infrastructure evolves in tandem with the organization's expansion. Addressing scalability challenges provides valuable insights for businesses looking to enhance their monitoring and automation capabilities as they grow.

Finally, technology fragmentation is a persistent issue, particularly in sectors like manufacturing, where operational technology (OT) and IT systems often coexist. The complexity of managing these disparate systems demands adaptive monitoring solutions that can integrate across different technologies. The ability to bridge the gap between OT and IT systems offers organizations a cohesive view of their entire infrastructure, while automation must navigate diverse technology stacks to ensure seamless management of incidents and events. Overcoming the fragmentation of technology is crucial for automating diagnostics and remediation processes, creating a more unified and efficient approach to monitoring in complex technological landscapes. [2][6]

6. BENEFITS OF MONITORING AND AUTOMATION

In today's dynamic business environment, operational efficiency is essential for ensuring smooth, uninterrupted processes. Monitoring and automation work in tandem to support this goal. Monitoring tools offer real-time visibility into systems, allowing organizations to anticipate issues such as performance bottlenecks or outages and take corrective action before disruptions occur. Automation complements this by handling routine, repetitive tasks with precision, executing predefined workflows that keep operations running smoothly and consistently. Together, they create a seamless operational rhythm that minimizes downtime and maximizes productivity.

Cost efficiency is another key benefit. Monitoring helps organizations identify and eliminate inefficiencies, such as underutilized resources, enabling smarter allocation and budget optimization. At the same time, automation reduces the need for manual labor, streamlining operations and significantly lowering operating costs. This not only boosts overall performance but also supports long-term financial sustainability.

Security is also greatly enhanced through the integration of monitoring and automation. Continuous monitoring detects threats and anomalies in real time, while automation ensures immediate response through predefined security actions. This proactive approach reduces risk exposure and minimizes potential damage. A prime example is a leading U.S. investment bank, which integrated monitoring and automation tools to swiftly neutralize threats, thereby strengthening its digital defenses.

Finally, these tools empower organizations to be more adaptable in the face of change. As industries evolve and technologies shift, monitoring and automation provide the flexibility and speed needed to adjust. By anticipating disruptions and enabling rapid response, they help businesses stay ahead of challenges and navigate transformation with confidence.

In essence, the combined power of monitoring and automation drives operational excellence, cost savings, robust security, and agility - key ingredients for thriving in an ever-changing landscape.[2]

7. FUTURE OF SIEM SYSTEMS

The future of Security Information and Event Management (SIEM) systems is being shaped by political, economic, societal, technological, and environmental factors. Governments, especially in the EU, are prioritizing cybersecurity as a national security and economic issue, leading to increased investments in cybersecurity infrastructure and innovation. This push is expected to accelerate the adoption and development of SIEM systems, which are central to protecting digital ecosystems. The growing emphasis on regulatory requirements for interoperability, scalability, and cost-effectiveness is driving the advancement of more sophisticated SIEM technologies.

Economically, the rise of remote workforces and freelance employment models is changing how organizations manage data and access security. As the workforce becomes more flexible, SIEM systems must adapt to diverse user profiles and endpoints, often beyond traditional security perimeters. This shift requires platforms to be more flexible, with intuitive interfaces capable of analyzing varied user behaviors while maintaining visibility and control. Additionally, globalization continues to expand organizational networks, making IT environments more complex. SIEM systems must be scalable to meet these challenges, ensuring effective security monitoring across distributed infrastructures. Smaller businesses, which often lack the resources for robust cybersecurity, are increasingly driving demand for affordable, accessible SIEM solutions.

From a societal perspective, the growing reliance on digital technologies and constant connectivity emphasizes the importance of robust cybersecurity strategies. Younger generations, who are more aware of digital risks, are demanding transparency and accountability in security practices. Social media also plays a dual role as both a risk vector and an intelligence source. SIEM systems must be able to analyze large volumes of online discourse, detecting potential threats from the flow of information. Moreover, high-profile cyber-attacks, especially those targeting critical infrastructure, highlight the need for SIEM systems capable of detecting and responding to advanced threats quickly.

Technologically, the widespread adoption of cloud computing is transforming how organizations store, access, and process data. Cloud-native SIEM platforms benefit from increased scalability and computing power, enabling faster detection and analysis of security events across distributed environments. Mobile technologies and the Bring Your Own Device (BYOD) trend add complexity to security management, requiring SIEM systems to monitor risks from unmonitored endpoints, unpatched software, and unencrypted data. Additionally, the explosion of data from the Internet of Things (IoT) presents both challenges and opportunities, pushing SIEM platforms to evolve into powerful analytics engines capable of processing vast datasets in real time. The introduction of 5G networks will only amplify this challenge, requiring SIEM systems to handle greater volumes and speeds of data.

In response, SIEM platforms are increasingly integrating artificial intelligence (AI) and machine learning. These technologies enable predictive analysis and enhance the ability to detect anomalies in user behavior and network

activity. AI-driven SIEM systems can process vast datasets more efficiently than human analysts, reducing false positives and speeding up the response cycle. When combined with Security Orchestration, Automation, and Response (SOAR), AI-driven systems can autonomously take defensive actions and prioritize alerts, adapting to evolving threats. The integration of unsupervised learning models could further improve anomaly detection by establishing dynamic baselines, allowing for faster, more accurate identification of deviations and more targeted responses to potential security breaches.

As SIEM systems become more self-tuning and context-aware, the role of human analysts may shift from direct monitoring to overseeing and auditing automated security operations. Additionally, integrating social media analytics and behavioral data into SIEM strategies could enhance threat intelligence, enabling more proactive and accurate threat detection.

In conclusion, SIEM systems are evolving into proactive, intelligent components of organizational resilience. As political, economic, societal, and technological factors intersect, SIEM systems are moving beyond passive monitoring to become critical, proactive tools in cybersecurity. The future of SIEM will depend on its ability to absorb complexity, streamline responses, and deliver actionable insights quickly and accurately across dynamic digital environments. This transformation will ensure that SIEM systems remain essential in the ever-changing landscape of cybersecurity.[4] [5]

8. EMPOWERING CYBERSECURITY WITH ADVANCED ARTIFICIAL INTELLIGENCE TECHNOLOGIES

AI and machine learning are becoming increasingly important in cybersecurity as threats grow more complex. While these technologies offer considerable promise, especially in machine learning and natural language processing, they should not be seen as a one-size-fits-all solution. Security professionals need to combine AI with traditional methods to manage cyber risks effectively. As the demand for AI in cybersecurity rises, it's vital to make informed choices on its use to protect organizations.

The cybersecurity landscape is under more pressure as businesses consolidate onto fewer platforms, creating an interconnected attack surface. Hybrid work models and collaboration tools like Microsoft Teams and Slack have widened vulnerabilities, making organizations more vulnerable to targeted attacks. The consolidation of digital tools and the high value of mass data has made major providers more attractive targets, raising the risk and cost of data breaches. These changes have led to more sophisticated attacks, undermining traditional human defenses.

AI offers key benefits, such as processing vast data quickly, making smarter decisions over time, and automating tasks. However, it's important to remember that AI is just a tool and must be integrated into broader defense strategies. Generative AI, for example, has been used by malicious actors to craft more convincing phishing emails, contributing to the rise in such attacks. While the full impact of generative AI is still unfolding, its role in increasing cybersecurity threats is evident.

In cybersecurity, decisions on what to allow, block, or address are critical. AI can provide quicker, more efficient responses

to these questions at scale, but must be part of a comprehensive defense strategy. Leading security providers use AI to bolster defenses, neutralize threats, and lighten the load on security teams. However, AI performs best when paired with traditional methods, enhancing detection and improving security.

Machine learning requires careful application, supported by expertise and quality data. As AI technologies advance, they also make cyberattacks more sophisticated. To stay ahead of cybercriminals, AI must be used effectively and integrated into multi-layered defense strategies. It should be deployed in areas with large datasets, like anomaly detection, and supported by continuous feedback loops to improve its performance. Human expertise is vital to refining AI security measures, ensuring greater accuracy and adaptability.

The effectiveness of AI in cybersecurity depends on high-quality data and proper human oversight. Poor data or incorrect decisions during development can lead to flawed results, highlighting the importance of data quality and human guidance in achieving reliable AI-driven security.

AI is already a crucial part of multilayered cybersecurity solutions, vital for protecting communications, people, and data. Its deployment should be strategic, focusing on areas where AI's strengths can be fully utilized while addressing its limitations.

While AI's role in cybersecurity continues to expand, its full potential is still being understood. The future remains uncertain, but the possibilities for AI are vast, driven by the expertise of those working to harness its capabilities. Time will reveal the full extent of its impact. [5][7]

9. CONCLUSION

The importance of infrastructure monitoring in safeguarding critical infrastructures cannot be overstated. As modern IT systems grow increasingly complex and vulnerable to cybersecurity threats, the need for advanced monitoring tools becomes imperative. The evolution of monitoring solutions has been pivotal in improving system performance, security, and reliability. Looking to the future, SIEM systems are poised to evolve into even more sophisticated platforms. These systems will likely integrate deeper analytical capabilities, harnessing the power of Artificial Intelligence to provide real-time threat intelligence and predictive insights. With the growing need to process vast amounts of data quickly, future SIEM solutions will focus on scalability, adaptability, and automation, making them indispensable in managing increasingly dynamic cybersecurity landscapes.

Furthermore, the role of Artificial Intelligence in cybersecurity will continue to expand, reshaping how organizations protect their critical infrastructures. AI will enhance the ability to identify anomalies and threats that traditional systems may overlook, offering unparalleled speed and accuracy in detecting potential breaches. As AI and Machine Learning progress, their contributions to cybersecurity will extend beyond monitoring; they will play a pivotal role in risk assessment, response automation, and strategic decision-making.

By combining advancements in SIEM systems with the transformative capabilities of AI-driven technologies, organizations can proactively address emerging risks, ensure resilience, and maintain the integrity of critical infrastructures. These innovations will remain at the forefront of cybersecurity, guiding industries toward a more secure and efficient future.

10. REFERENCES

- [1] Habib Badawi, Cybersecurity: Emerging trends and challenges: https://journal.scsa.ge/wp-content/uploads/2024/11/0039_cybersecurity-emerging-trends-and-challenges.pdf Published: November 2024.
- [2] NiCE IT Management Solutions GmbH: Navigating Industry-Specific Challenges in Infrastructure Monitoring and Automation, A White Paper by NiCE IT Management Solutions, March 2024 <https://www.nice.de/wp-content/uploads/2024/03/Monitoring-and-Automation-Whitepaper-by-NiCE-2024Q1.pdf> Published: March 2024.
- [3] Will Kelly, Emily Foster: Compare 8 tools for IT monitoring in 2025, Published: 20 December 2024 <https://www.techtarget.com/searchitoperations/feature/Compare-8-tools-for-IT-monitoring> Published: March 2024.
- [4] González-Granadillo, G.; González-Zarzosa, S.; Diaz, R.: Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures, Sensors, 2021 https://www.researchgate.net/publication/353214895_Security_Information_and_Event_Management_SIEM_Analysis_Trends_and_Usage_in_Critical_Infrastructures (accessed Jan. 30, 2025)
- [5] mimecast: White Paper AI and Cybersecurity: The Promise and Truth of the AI Security Revolution, 2024 <https://www.mimecast.com/resources/white-papers/ai-and-cybersecurity/> (accessed Jan. 25, 2025)
- [6] Alexandr Bandurchin, What is Infrastructure Monitoring? <https://uptrace.dev/glossary/what-is-infrastructure-monitoring> (accessed Mar. 22, 2025)
- [7] Alexandr Bandurchin, What is Best DataDog Competitors in 2025 <https://uptrace.dev/blog/datadog-competitors> (accessed Mar. 20, 2025)
- [8] González-Granadillo, G.; González-Zarzosa, S.; Diaz, R.: Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures, Sensors, 2021, Page: 6, https://www.researchgate.net/publication/353214895_Security_Information_and_Event_Management_SIEM_Analysis_Trends_and_Usage_in_Critical_Infrastructures (accessed Mar. 22, 2025).