electronics

MDPI

Article

Navigating the CISO's Mind by Integrating GenAI for Strategic Cyber Resilience

Šarūnas Grigaliūnas [1,*,†], Rasa Brūzgienė [2,†], Kęstutis Driaunys [2], Renata Danielienė [2], Ilona Veitaitė [2], Paulius Astromskis [2], Živilė Nemickienė [2], Dovilė Vengalienė [2], Audrius Lopata [3], Ieva Andrijauskaitė [4] and Neringa Gaubienė [4]

[1] Kaunas University of Technology, Department of Computer Sciences, Studentu Str. 50, 51368 Kaunas, Lithuania

[2] Vilnius University, Kaunas Faculty, Muitinės Str. 8, 44280 Kaunas, Lithuania; rasa.bruzgiene@knf.vu.lt (R.B.); kestutis.driaunys@knf.vu.lt (K.D.); renata.danieliene@knf.vu.lt (R.D.); ilona.veitaite@knf.vu.lt (I.V.); paulius.astromskis@knf.vu.lt (P.A.); zivile.nemickiene@knf.vu.lt (Ž.N.); dovile.vengaliene@knf.vu.lt (D.V.)

[3] Kaunas University of Technology, Department of Information Systems, Studentu Str. 50, 51368 Kaunas, Lithuania; audrius.lopata@ktu.lt

[4] Vilnius University, Faculty of Law, Saulėtekio al. 9, 10222 Vilnius, Lithuania; ieva.andrijauskaite@tf.stud.vu.lt (I.A.); neringa.gaubiene@tf.vu.lt (N.G.)

* Correspondence: sarunas.grigaliunas@ktu.lt

† These authors contributed equally to this work.

Abstract: AI-driven cyber threats are evolving faster than current defense mechanisms, complicating forensic investigations. As attacks grow more sophisticated, forensic methods struggle to analyze vast wearable device data, highlighting the need for an advanced framework to improve threat detection and responses. This paper presents a generative artificial intelligence (GenAI)-assisted framework that enhances cyberforensics and strengthens strategic cyber resilience, particularly for chief information security officers (CISOs). It addresses three key challenges: inefficient incident reconstruction, open-source intelligence (OSINT) limitations, and real-time decision-making difficulties. The framework integrates GenAI to automate routine tasks, the cross-layering of digital attributes from wearable devices and open-source intelligence (OSINT) to provide a comprehensive understanding of malicious incidents. By synthesizing digital attributes and applying the 5W approach, the framework facilitates accurate incident reconstruction, enabling CISOs to respond to threats with improved precision. The proposed framework is validated through experimental testing involving publicly available wearable device datasets (e.g., GPS data, pairing and activity logs). The results show that GenAI enhances incident detection and reconstruction, increasing the accuracy and speed of CISOs' responses to threats. The experimental evaluation demonstrates that our framework improves cyberforensics efficiency by streamlining the integration of digital attributes, reducing the incident reconstruction time and enhancing decision-making precision. The framework enhances cybersecurity resilience in critical infrastructures, although challenges remain regarding data privacy, accuracy and scalability.

Keywords: GenAI; cyberforensics; CISO; OSINT; digital attributes; 5W

check for updates

Academic Editor: Krzysztof Szczypiorski

Received: 3 February 2025
Revised: 15 March 2025
Accepted: 24 March 2025
Published: 27 March 2025

Citation: Grigaliūnas, Š.; Brūzgienė, R.; Driaunys, K.; Danielienė, R.; Veitaitė, I.; Astromskis, P.; Nemickienė, Ž.; Vengalienė, D.; Lopata, A.; Andrijauskaitė, I.; et al. Navigating the CISO's Mind by Integrating GenAI for Strategic Cyber Resilience. *Electronics* **2025**, *14*, 1342. https://doi.org/10.3390/electronics14071342

1. Introduction

The digitization of services, the adoption of new technologies and the inclusion of members of society in the digital space are proceeding faster than the assessment of cyber threats and the selection of appropriate mitigation tools and techniques. This gap facilitates the exploitation of existing vulnerabilities for cybercrime, and the rapid evolution of technologies such as artificial intelligence (AI) or generative artificial intelligence (GenAI) makes them powerful tools in the hands of malicious actors. According to the Lithuania National Cyber Security Centre's 2023 National Cyber Security Status Report [1], the development of threats from local and global criminal structures, ranging from social engineering to serious threats to both national security and information and communication technology (ICT) infrastructures, is a major concern for the global security community due to the potential use of AI technologies for cyberattacks. According to the ENISA Artificial Intelligence and Cybersecurity Research study [2], malware is increasingly using AI to enhance its effectiveness and efficiency by enhancing its ability to evade detection, adapt to changing environments, target specific vulnerabilities and propagate and persist on target systems. AI-driven malware leverages reinforcement learning to enhance attack effectiveness and adaptability. These findings suggest that generative AI is actively involved in cyberattacks, posing a significant security risk.

Within the realm of cyber security, the European Parliament adopted the European AI strategy [3,4], stating that it is already filling—or assisting with—a number of roles and processes. It is being used to analyze logs, predict threats, read source code, identify vulnerabilities and even create or exploit vulnerabilities, such as during penetration testing. In this context, the chief information security officer (CISO) has a key role in the implementation and success of the EU AI strategy in addressing AI-assisted challenges. As cybercrime continues to evolve and take new forms, the CISO must be adequately equipped to assess cyber threats, identify cybercrime and conduct effective investigations. The evolving cyber landscape necessitates that CISOs rethink preparedness. Tasked with remediating, mitigating or transferring the risks posed by complex threats, the CISO is at the forefront of implementing critical security controls, organizing incident response strategies and ensuring robust business continuity and disaster recovery capabilities. In addition, the CISO is entrusted with the crucial task of anticipating future security challenges and planning the organizational and technical measures to ensure cyber resilience accordingly.

Following the CISO Workforce and Headcount 2023 Report [5], CISOs are in high demand as cybersecurity professionals, but there is a significant global shortage. Generative AI supports CISOs in cybersecurity by automating routine tasks, improving threat detection and providing advanced forensic tools. Research on generative AI-assisted CISO functions is emerging and rapidly evolving [6,7]. It offers exciting opportunities for innovation and significant advancements in cybersecurity practices. GenAI refers to a category of AI models that generate new content or insights from various data sources, encompassing not only large language models (LLMs) but also multimodal models that integrate text, images and structured data processing. Generative AI uses neural networks trained on large datasets, integrating cybersecurity data across silos. Although LLMs are primarily focused on natural language understanding and generation, GenAI employs a wider range of AI-driven methodologies for cyberforensics, including structured data synthesis and digital attribute analysis. The use of GenAI rather than LLMs allows for more comprehensive incident reconstruction, as it integrates diverse data types beyond text-based insights. This can give CISOs a more natural method for identifying, synthesizing and summarizing insights [8,9]. The novelty of this research area is underscored by the recent GenAI technological advancements and the evolving threat landscape that necessitates advanced solutions [10]. As such, it is an area of high interest and potential within both the academic and professional cybersecurity communities. By leveraging generative AI assistance in the routine tasks of the CISO, organizations can improve threat detection and response, optimize resources, ensure compliance, enhance training programs and make more informed strategic decisions [11]. These benefits underscore the transformative potential of generative AI in the realm of cybersecurity, opening a wide window for future research and development.

On the other hand, the growth of wearable technology has increased the need for specialized cyberforensics methods that can effectively identify and reconstruct cybercrime involving such devices [12]. Given that wearable devices operate in diverse environments—ranging from personal use in fitness and healthcare to enterprise and industrial applications—the cybersecurity risks vary significantly depending on factors such as data transmission methods, connectivity settings (e.g., Bluetooth, Wi-Fi, cellular networks), and regulatory constraints. These environmental variables influence forensic investigations by affecting data accessibility, storage conditions, and potential attack vectors, making it imperative to develop adaptable and context-aware forensic methodologies.

Although AI is widely used in cybersecurity, many AI models function as opaque systems, limiting transparency and interpretability [13]. This deficiency decreases the confidence of human users in the models used for cyber defense, especially as cyberattacks become increasingly diverse and complicated. While explainable AI (XAI) has been increasingly explored in cybersecurity applications such as malware detection, intrusion detection and network security, a significant gap remains in its application to cyberforensics. Specifically, there is limited research on integrating XAI-driven methodologies into forensic investigations involving wearable devices, where explainability is crucial for enhancing the transparency of digital evidence analysis and supporting CISO decision-making processes. Despite their potential, existing cyberforensics approaches lack a comprehensive generative AI-driven methodology to integrate and enhance cyberforensics investigations across different layers of digital evidence. This gap is especially evident in wearable devices, where data originates from both the application and the network layers, making it difficult to form a complete picture of malicious events. The current separation between network forensics and application forensics results in a fragmented understanding of malicious events.

Additionally, traditional methods lack AI-enhanced capabilities which could streamline the interpretation of evidence and assist CISOs in building a more cohesive narrative of incidents [14]. Therefore, there is a crucial need for an integrated GenAI-assisted approach that can cross-layer digital evidence, providing a more effective solution for the complex challenges in wearable device cyberforensics. Such a GenAI-assisted approach also has the potential to incorporate open-source intelligence (OSINT) to identify malicious activities and infer the behavior and personality of potential attackers by analyzing attributes from wearable device owners. This capability provides deeper insights under the *Who-When-What-Why-Where* (5W) umbrella, offering CISOs a holistic view of cyber incidents by building more detailed behavioral profiles of potential attackers, drawing connections between digital evidence from wearable devices and OSINT sources. This integration of personality attributes and digital forensics allows for more targeted threat mitigation strategies, strengthening the overall security posture.

This study addresses the following research questions:

- RQ1: How can a GenAI-assisted framework be developed to enhance the accuracy and comprehensiveness of cyberforensics in wearable devices by effectively integrating and cross-layering digital evidence between the network and application domains?
- RQ2: How can this framework, through the integration of OSINT, identify and reconstruct a malicious incident while providing a holistic view of the incident under the 5W umbrella?

RQ1 is important due to the growing role of wearables in cyber incidents and the limitations of traditional forensic methods in analyzing the data. Traditional techniques treat the network and application layers separately, resulting in fragmented analyses. A GenAI-powered framework bridges this gap by synthesizing digital evidence across sources, improving forensic accuracy. This research strengthens cyber resilience by using wearable data to detect cybercrime, insider threats and anomalies. As wearables are increasingly used in critical sectors such as healthcare, defense and finance, securing their data is essential for robust forensic capabilities. RQ2 focuses on cyberforensic capabilities by integrating OSINT for deeper contextual insights. OSINT enhances situational awareness by correlating wearable data with public intelligence, enriching forensic investigations. The 5W approach structures incident reconstruction, linking numerical evidence to real-world events for better decision making. Systematic OSINT analysis provides actionable intelligence, aiding CISOs in managing complex threats. Despite its advantages, the framework still faces limitations in addressing key CISO challenges, such as incident prioritization, compliance and resource constraints.

The aim of this research is to answer the above listed research questions by developing a GenAI-assisted framework for cyberforensics that improves the detection of the associated attributes and reconstruction of malicious events involving wearable devices. By cross-layering attributes from both the network and application domains and combining them with OSINT data, this framework seeks to comprehensively answer the 5W questions in order to provide a holistic understanding of incidents. This research aims to enhance the efficiency and accuracy of cyberforensics processes, enabling detailed reconstruction of incidents through GenAI-assisted pattern recognition, particularly for incidents involving wearable technologies. This aim will be achieved by focusing on the following:

- How to develop an GenAI-assisted methodology for cross-layered evidence synthesis in cyberforensics;
- How to design an OSINT integration process for wearable device data analysis, thus creating a more complete understanding of malicious incidents involving wearable devices;
- How to validate the GenAI-assisted framework using real-world case studies or datasets to demonstrate identification of malicious activities and the behavioral profiling of potential attackers;
- How to address the current limitations in cyberforensics by bridging the gap between different forensic layers and integrating AI-driven insights, ultimately supporting CISOs in improving cyber resilience and preparedness.

The results of this work will support CISOs in managing security incidents more effectively, ensuring robust preparedness and mitigating threats involving wearable technologies as a part of a broader strategy for cyber resilience of critical infrastructure. Additionally, by integrating the GenAI-assisted cyberforensics framework into security operations centers (SOCs), organizations can enhance real-time threat detection, incident response automation and forensic investigation efficiency, thereby strengthening cyber resilience in critical infrastructure.

2. Related Research

This study is a part of the ongoing research in a research project titled "Research on Cyber Resilience Through Application of Generative Artificial Intelligence in Chief Information Security Officer Operations". This project directly addresses the first objective of the second goal of the Lithuanian Cybersecurity Strategy [15] ("to develop the state's capabilities and capacities to fight against criminal acts in cyberspace") by creating an adaptive security system based on the assistance of GenAI capabilities for understanding and reacting to threats as a CISO's proactive tool to fight against cybercrime.

Several innovative projects represent the current status of related research in the fields of AI and cybersecurity within the EU. AI4CYBER [16] focuses on developing trustworthy cybersecurity services using AI and big data technologies. KINAITICS [17] aims to explore new attack opportunities offered by AI-based systems by developing tools and methodologies combining behavioral monitoring with cybersecurity tools to protect against

AI-driven cyber threats. ResilMesh [18] creates a cyber-situational awareness-based security orchestration and analytics platform architecture (SOAPA) with the goal of improving digital infrastructure resilience and assisting CSIRTs in building cyber resilience capacity. SYNAPSE [19] focuses on developing an integrated cybersecurity risk and resilience management platform that encompasses incident response, AI-enhanced situational awareness, preparedness and risk management. PHOENiX [20] develops a cyber resilience framework with AI-assisted orchestration and automation for incident response and information exchange which is tailored to essential service operators and the national authorities from EU member states.

However, there are no current scientific projects which directly address the aim of this research. The existing research on explainable artificial intelligence (XAI) in cybersecurity highlights several advantages that are directly relevant to CISO functions. In a comprehensive survey on XAI for cybersecurity, researchers emphasized the importance of interpretable models in facilitating trust and transparency when deploying AI-driven security solutions [21]. The work in [21] highlights how explainable models improve decision-making processes by providing CISOs with insights into how AI systems classify threats and generate alerts. Furthermore, it underscores the necessity of XAI for regulatory compliance, as transparency in AI decision making aligns with global data protection laws and cybersecurity governance frameworks. However, the survey also identified challenges, such as the computational complexity of explainable models and the potential trade-off between interpretability and model accuracy.

Another study [22] investigated the application of XAI in cybersecurity, focusing on its role in identifying vulnerabilities and improving threat detection. The findings suggest that while XAI improves the interpretability of AI-generated threat intelligence, it also introduces potential security risks. Attackers can exploit explainability features to reverse-engineer security mechanisms, creating adversarial threats that compromise AI-driven cybersecurity defenses. For CISOs, this raises concerns about balancing the need for transparency with the requirement to maintain robust and resilient security infrastructures. The study under discussion also points out that current XAI frameworks lack standardized methodologies for implementation, making it difficult for CISOs to adopt explainability solutions seamlessly across various security tools and platforms.

A third body of research [23] explored the intersection of XAI and generative AI (GenAI) in cybersecurity, examining how explainability techniques can enhance AI-driven security automation. The study proposes that while GenAI improves the efficiency of cybersecurity operations by automating threat detection, digital forensics and incident response, its lack of interpretability remains a significant barrier to adoption in high-stakes security environments. The research highlights that CISOs require explainable GenAI models to justify security decisions, validate AI-generated insights and mitigate the risks associated with AI bias and hallucinations. Despite its advantages, the above study identified limitations such as the increased processing overhead required for explainability and the challenges of integrating XAI into deep learning-based cybersecurity solutions.

The increasing prevalence of wearable devices in various sectors, particularly healthcare and personal fitness, necessitates a robust forensic strategy to address the unique challenges posed by these technologies. Wearable devices, such as smartwatches and fitness trackers, collect sensitive user data, which can be crucial in forensic investigations. However, forensic examination of these devices is complicated by their architecture and the nature of the data they store. The complexity of IoT malware and the limitations of current forensic methodologies are highlighted in another work [24]. The authors identified research gaps, including the need for comprehensive IoT-specific datasets, integration of interdisciplinary methods and scalable real-time detection solutions. The review emphasizes the necessity for advanced countermeasures against anti-forensic techniques, indicating a lack of integrated approaches in current methodologies.

Researchers [25] elaborated on the unique challenges in IoT forensics, noting that current investigation techniques struggle with evidence collection and preprocessing due to counter-analysis techniques and difficulties in gathering data from devices and the cloud. Their work also points out procedural problems with preparedness, reporting and presentation, suggesting a lack of holistic approaches in current forensic practices.

While not directly addressing GenAI's role in forensics, another team of researchers presented a promising direction for improving digital forensics analysis [26]. They proposed a reproducible set-up for information extraction using NLP, which could potentially be extended to incorporate GenAI capabilities. This approach aims to decrease the time required for human supervision and review, addressing the current inability of tools to synthesize data and produce multi-layered evidence efficiently.

Another team of authors [27] highlighted the challenges in the examination, acquisition, identification and analysis of data from smartwatches, emphasizing the need for a methodology that ensures forensically sound data acquisition from these devices. Similarly, others discussed the forensic artifacts stored by devices like the Fitbit Versa 2 and the privacy concerns associated with the data collected, underscoring the importance of understanding the storage mechanisms of wearable devices [28]. Moreover, the security of wearable devices is paramount, given their role in transmitting sensitive health information.

Another researcher [29] discussed essential security parameters—confidentiality, integrity, authenticity and availability (CIAA)—which must be upheld to prevent breaches that could compromise device security. This is echoed in another work [30] which compared encryption algorithms suitable for wearable devices, highlighting the necessity of implementing robust cryptographic protocols to secure data transmission. The integration of advanced security measures, such as federated learning and blockchains, has been proposed to enhance the security and privacy of wearable IoT devices in predictive healthcare, as demonstrated in [31].

In terms of cyber resilience, organizations must adopt a proactive approach that incorporates the unique characteristics of wearable devices into their cybersecurity strategies. This includes developing lightweight authentication protocols tailored to resource-constrained wearable devices, as suggested in [32], which addressed vulnerabilities such as replay attacks and impersonation. Furthermore, the implementation of physical, unclonable functions for authentication, as proposed by the researchers in [33], offers a promising avenue for enhancing security in wearable computing environments. The forensic landscape surrounding wearable devices is evolving, and it is crucial for chief information security officers to stay informed about these developments. The need for a comprehensive strategy that encompasses both forensic analysis and cybersecurity measures is essential for ensuring the integrity and security of data collected by wearable devices. By integrating GenAI into the cybersecurity functions of CISOs, new benchmarks in threat anticipation, automated system responses and intelligent threat management will be set, paving the way for resilient cyber ecosystems which adapt to new threats as they emerge. Given the current technological advances in artificial intelligence and cyber security, the expected results of integrating GenAI into CISOs' operations are important for the development of new information security standards and practices, which will have a significant impact on future innovations in this field.

However, despite these advancements, the existing research does not sufficiently explore the role of GenAI in extracting and analyzing digital evidence from wearable technologies. The current literature primarily focuses on traditional AI techniques for threat detection and forensic investigations, often neglecting the potential of GenAI to automate and enhance the accuracy of cyberforensics. The ability to synthesize wearable device data across different layers—such as network traffic, sensor logs, and user activity—combined with GenAI-driven capabilities tailored to CISOs presents an opportunity to significantly improve cyber resilience. This research aims to address these gaps by developing a framework which integrates GenAI for automated forensic analysis of wearable devices while ensuring that security leaders can make informed, data-driven decisions in response to emerging cyber threats.

3. GenAI-Assisted Framework for Cyberforensics

3.1. Framework Architecture and Components

The concept of GenAI-assisted cyberforensics for data collected from wearable devices leverages generative artificial intelligence to enhance the analysis and interpretation of data from modern cyber environments (Figure 1).

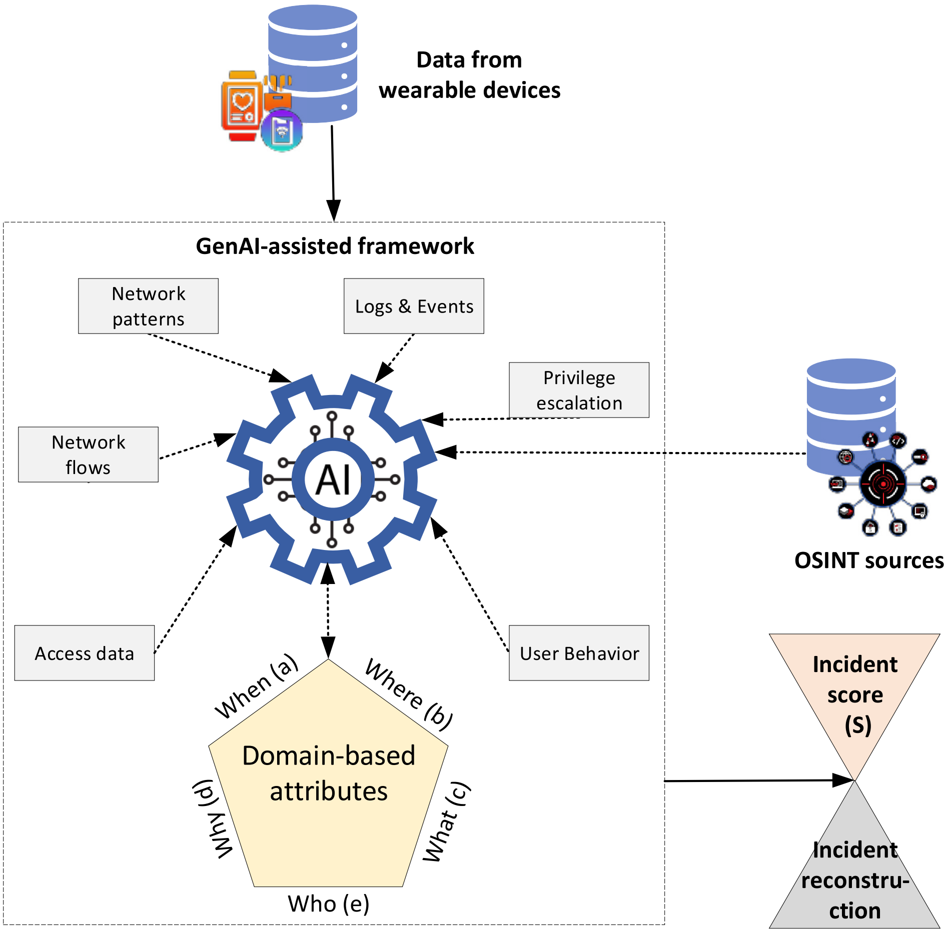

Figure 1. Concept of GenAI-assisted cyberforensics for data collected from the wearable devices.

In this framework, GenAI plays a central role in processing data. GenAI is a subset of deep learning, as it uses artificial neural networks and can process labeled and unlabeled data using supervised, unsupervised and semi-supervised methods. Unlike traditional LLMs, which focus primarily on natural language, the used GenAI model integrates structured forensic data processing, temporal sequence modeling and cross-modal embeddings to align information from multiple sources, including wearable device logs and open source intelligence (OSINT). Specifically, a multimodal transformer architecture was optimized for forensic event reconstruction and anomaly detection. Said transformer architecture, which is similar to vision-language transformers (ViLTs) and BERT-based models, enables the GenAI-assisted system to extract contextual relationships, model temporal dependencies and improve incident reconstruction accuracy, ultimately enhancing cyberforensic decision making. In this case, it allows assisting CISOs in detecting and responding to cybersecurity incidents.

Wearable devices generate extensive biometric and sensor data, spanning both the network and application domains. GenAI uses this multimodal data, extracts the digital attributes and associates them with the corresponding source category: network traffic, network pattern, system logs and events, access, user behavior or privilege escalation. Following this process, the 5W questions are used for identification and listing of the cross-related and cross-layered digital attributes (Figure 2).

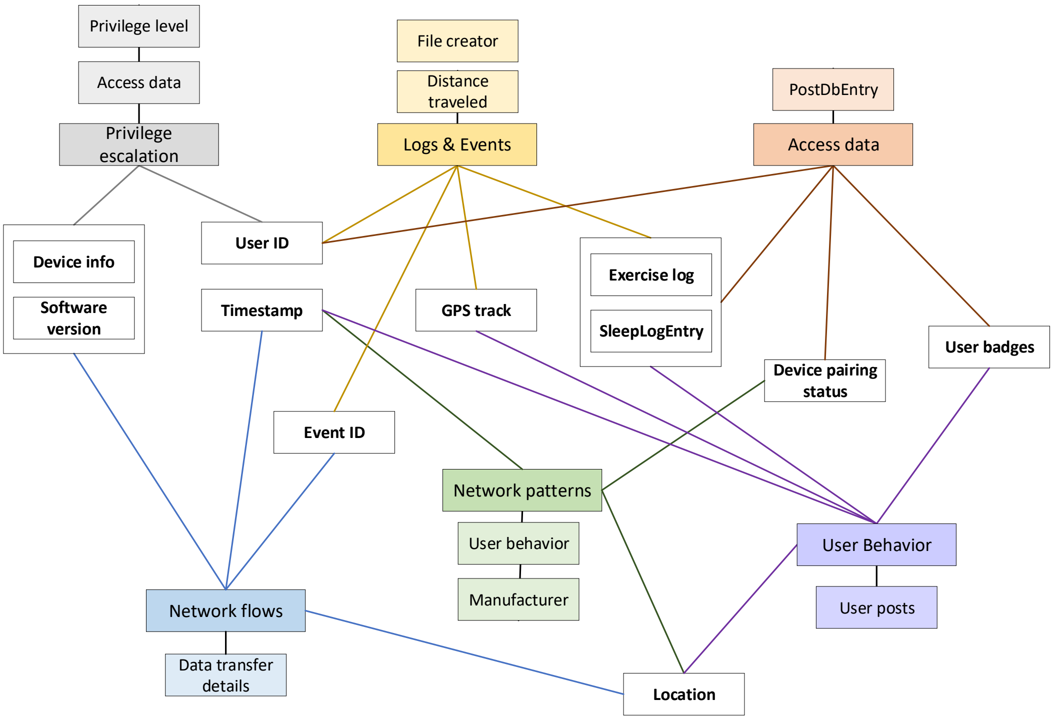

Figure 2. Cross-layered attributes through the network and application domains.

The ability to synthesize these digital attributes with data from OSINT inputs allows for comprehensive understanding of an incident. The interconnection between the components in the GenAI-assisted framework is crucial for its effective operation. As illustrated in Figure 2, the framework integrates data from various domains, creating a cohesive analysis environment. The cross-layered attributes shown in the figure are not isolated data points but form an interconnected network of evidence which GenAI processes simultaneously. The device information (such as the device info and software version) directly influences how the user ID and access data are interpreted in the who component while simultaneously affecting the reliability assessment of GPS tracks in the where component. Similarly, timestamp data serve as a temporal anchor connecting the when component to event sequences in the what component through exercise log and sleep log entry data. This interconnectivity pertains to the correlation between privileged access events, network flows and user behavior patterns. When GenAI identifies anomalies in network patterns, it autonomously cross-references these with privileged access events to ascertain whether suspicious escalations are transpiring. The framework's efficacy is rooted in its capacity to acknowledge that these ostensibly diverse data points—from network traffic to user posts—constitute various aspects of the same security picture. The incorporation of OSINT further augments these relationships by supplying external context to internal data patterns, allowing the framework to differentiate between typical behavioral fluctuations and a possibly harmful activity. This complete approach guarantees that no one attribute is examined in isolation but rather as a part of an overarching security posture evaluation grounded in the 5W methodology.

3.2. The 5W Approach for Attribute Analysis and Scoring

GenAI assigns an incident score to each detected incident based on analysis of the collected data. The incident score S helps security leaders prioritize responses, as it evaluates the severity and context of a cybersecurity event by combining the domain-based attributes of five key components: when (a), where (b), what (c), why (d) and who (e)—as well as data from OSINT. Each component is assigned a weight, and the score is adjusted based on the dependencies between these 5W factors (Figure 3).

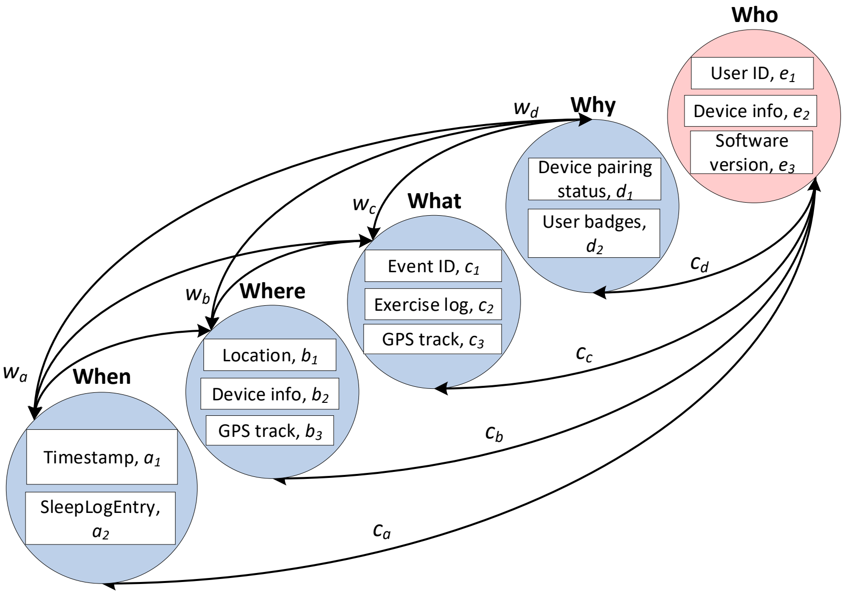

Figure 3. Dependencies of attributes between 5W factors.

Taking all components and dependencies into account, the formula can be expressed as shown in Equation (1):

$$S = \frac{f(w(a), w(b), w(c), w(d), w(e))}{\sum_{i \neq x} c_i \cdot w_i + f(\text{OSINT})} \tag{1}$$

where $f(w(a), w(b), w(c), w(d), w(e))$ is the base function for the weighted factors of when, where, what, why, and who, respectively, c_i is the dependency coefficient between component x and component i, w_i is the weight of component i, for which $i \in \{\text{When, Where, What, Why, Who}\}$ except x, and $f(\text{OSINT})$ adds additional weight based on external intelligence, validating or modifying the incident score based on news, social media or public records.

When $w(a)$ depends on attributes a_1 and a_2 and its relationships with the other components, as shown in Equation (2):

$$w(a) = f(a_1, a_2) + c_b \cdot w(b) + c_c \cdot w(c) + c_d \cdot w(d) \tag{2}$$

Where $w(b)$ depends on attributes b_1, b_2 and b_3 and its relationships with the other components, as shown in Equation (3):

$$w(b) = f(b_1, b_2, b_3) + c_a \cdot w(a) + c_c \cdot w(c) + c_d \cdot w(d) \tag{3}$$

What $w(c)$ depends on attributes c_1, c_2 and c_3 and its relationships with the other components, as shown in Equation (4):

$$w(c) = f(c_1, c_2, c_3) + c_a \cdot w(a) + c_b \cdot w(b) + c_d \cdot w(d) \tag{4}$$

Why $w(d)$ depends on attributes d_1 and d_2 and its relationships with the other components, as shown in Equation (5):

$$w(d) = f(d_1, d_2) + c_a \cdot w(a) + c_b \cdot w(b) + c_c \cdot w(c) \tag{5}$$

Who $w(e)$ depends on all of the previous components (when a, where b, what c and why d) and subfactors e_1, e_2 and e_3, as shown in Equation (6):

$$w(e) = f(e_1, e_2, e_3) - b \cdot \log(x_{who}) + c_a \cdot w(a) + c_b \cdot w(b) + c_c \cdot w(c) + c_d \cdot w(d) \tag{6}$$

where b is the scaling factor for the logarithmic decay based on the rank of who (x_{who}).

The mathematical formulations of the 5W framework are directly integrated into the GenAI model's training and inference processes. The weights ($w(a)$, $w(b)$, $w(c)$, $w(d)$ and $w(e)$) and dependency coefficients (c_a, c_b, c_c and c_d) serve as parameterized inputs to the model's attention mechanisms, influencing how the transformer architecture allocates importance across different attributes during analysis. During the training phase, these parameters are optimized through a multi-component loss function $\mathcal{L}$ which combines cross-entropy loss for classification tasks and the mean squared error for numerical predictions, as shown in Equation (7):

$$\mathcal{L} = \alpha \cdot \mathcal{L}_{CE}(5W_{pred}, 5W_{actual}) + \beta \cdot \mathcal{L}_{MSE}(S_{pred}, S_{actual}) + \gamma \cdot \mathcal{L}_{reg} \tag{7}$$

where $\mathcal{L}_{CE}$ represents the cross-entropy loss measuring the accuracy of attribute classification, $\mathcal{L}_{MSE}$ evaluates the prediction accuracy of the incident scores and $\mathcal{L}_{reg}$ is a regularization term preventing overfitting. The hyperparameters α, β and γ balance these components based on their relative importance. The model's weight optimization process automatically adjusts the dependency coefficients between the 5W components based on empirical evidence from training data, enabling the GenAI to learn the complex interrelationships between different digital attributes. This integration ensures that the 5W formulations are not merely theoretical constructs but practical computational elements that guide the GenAI's learning process. As the model processes new incidents, these mathematically formulated relationships help prioritize attention to the most relevant attributes in complex scenarios. When analyzing wearable device data with unusual timestamps (the when component), the model automatically gives increased weight to corresponding location attributes (the where component) based on the learned dependency coefficient c_a. This allows the GenAI to make contextually appropriate inferences even with incomplete or noisy data, improving incident reconstruction accuracy. The final result after application of the proposed GenAI-assisted framework reflects both the key details of the incident and the broader context, helping investigators assess its potential impact. If a high-end wearable device is located near a reported robbery at a specific time and there are news articles that mention it, then the incident score will be higher. Conversely, if a basic feature phone is located in a public park with no reported incidents, then the incident score will be lower. Additionally, GenAI assists in reconstructing the sequence of events. By cross-referencing the identified digital attributes, the generative AI provides a detailed timeline of the incident, which aids forensic investigations and decision-making processes.

4. Experimental Use Case

The GenAI-assisted framework was tested with a different wearable devices to ensure its adaptability across different device ecosystems.

To effectively integrate GenAI into cyberforensics, it is essential to explicitly understand the technical details and limitations involved. The transformer architecture employed in this study includes GPT-based models, specifically GPT-4 and GPT-3.5, supplemented by domain-specific fine-tuning to enhance accuracy and reduce model hallucinations. The transformers employed are decoder-only models utilizing self-attention mechanisms capable of efficiently processing multimodal and textual cybersecurity datasets. The GenAI-assisted framework implementation leverages advanced transformer-based language models, specifically using the GPT-4 architecture with 175 billion parameters for optimal performance in handling complex cyberforensic tasks. For cross-layered attribute analysis and complex pattern recognition across disparate data sources, we fine-tuned the model on specialized cybersecurity datasets. The hardware requirements for optimal operation include high-performance computing capabilities, with our implementation utilizing an Apple MacBook Pro with an M4 CPU and 48 GB of RAM for development and testing. For enterprise-level deployment, we recommend dedicated GPU acceleration with at least 32 GB of VRAM to ensure real-time processing capability when handling large volumes of wearable device data and OSINT information simultaneously. The transformer's attention mechanisms are particularly effective at identifying correlations between network behavior patterns and application-level actions across devices, enabling deeper insights into potential security incidents than traditional rule-based systems.

The experimental scenarios included (1) identification and integration of cross-layered digital attributes (e.g., GPS data, pairing logs and activity logs) and (2) synthesis of OSINT inputs with device-generated data to enhance incident reconstruction accuracy.

4.1. Extraction of Attributes from Wearable Devices and OSINT Data

Specific questions tailored to the 5W approach and aligned with NIST SP 800-86 [34] were designed in order to extract and analyze digital attributes while integrating OSINT data. The questions addressed toward the GenAI model for the extraction of digital attributes from wearable devices are presented in Table 1.

Using the provided prompts, various digital attributes were systematically extracted from wearable devices to form a comprehensive cyberforensics analysis. The Who category revealed critical identifiers such as user IDs, device owners and their associated information (e.g., user ID, software version and privilege levels). Additionally, the logs captured data on who interacted with the devices during the timeframe of interest and highlighted unauthorized access attempts. The device pairing status was also scrutinized to determine who authorized connections and whether unauthorized pairing attempts occurred.

In the What category, detailed device attributes such as GPS tracks, activity logs, exercise logs and the device pairing status were analyzed, capturing specific events such as privilege escalations or unauthorized device interactions. Logs, such as the sleep log entry and exercise logs, provided key insights into user routines and any deviations from the expected behavior. The identification of the "what" component involved a multi-step analysis process. First, the GenAI model extracted the primary device attributes, such as GPS tracks, activity logs and the pairing status, from the raw data streams. Then, it performed pattern recognition to identify specific events (e.g., privilege escalations and unauthorized access attempts) by correlating event IDs with temporal and spatial metadata. This process was enhanced through the application of supervised learning techniques trained on labeled cybersecurity incident datasets, enabling the framework to distinguish between normal operational events and potentially malicious activities.

Table 1. Questions for the extraction of digital attributes from wearable devices.

5W Category	Questions for GenAI Model
Who	• Who is the owner of the device, and what is their associated user ID? • Who interacted with the device during the recorded timeframe, and were there any unauthorized access attempts? • Who authorizes device pairing, and how are unauthorized pairing attempts detected? • Who has access to the user ID and sensitive user records, and how is access logged and monitored?
What	• What device data were recorded (e.g., GPS tracks, activity logs and pairing status)? • What specific events were captured (e.g., pairing attempts and privilege escalations)? • What details about the device's manufacturer and model are recorded? • What types of logs are maintained for device pairing and location tracking, and how are they used to verify legitimate user activity versus malicious behavior?
When	• When were key activities recorded by the device (e.g., timestamp of data transfers and disconnections)? • When were software or firmware updates last applied to the device? • When are user activity logs (e.g., sleep data, exercise logs and GPS tracks) recorded? • When are GPS tracking functions activated?
Where	• Where was the device located based on GPS data during the event timeframe? • Where did the device establish connections, and were these locations consistent with legitimate activities? • Where are the location data captured and stored? • Where are user images and posts shared within applications? • Where does the device pairing log indicate connections were established, and are there signs of unauthorized devices being linked?
Why	• Why does the recorded device behavior deviate from typical usage patterns? • Why were certain device activities flagged as anomalous or suspicious? • Why might attackers target user activity logs or posts, and what value could these data provide to them? • Why are there discrepancies in recorded location or distance data?

For example, when analyzing the experimental dataset, the system identified unusual pairing attempts by detecting deviations in the device pairing status attribute combined with anomalous timestamps which fell outside typical user behavior patterns. The "What" attributes were then weighted according to their security significance using the mathematical formulations described in Equation (4), with higher weights assigned to critical security events like privilege escalations compared with routine activities.

The When category provided a critical timeline for understanding incidents, supported by timestamps associated with key activities such as data transfers, disconnections, GPS activations and user actions. The sleep log entry and exercise logs further complemented these timestamps by documenting user behavior during specific periods. The consistent recording of these logs allowed the framework to identify anomalies in usage patterns or detect activities occurring during unexpected hours, improving the timeline's precision.

For the Where category, the extracted GPS tracks and location data pinpointed the exact positions of the device during the event timeframe. The location attribute and device info from pairing logs were also crucial for identifying whether these locations were consistent with legitimate activities or linked to unauthorized connections. Analysis of the pairing logs provided further evidence of whether unauthorized devices were linked to specific geographic areas or flagged for unusual activity, helping to establish context for any deviations.

The Why category sought explanations for deviations in device behavior, including discrepancies in the recorded location, distance or activity logs. For example, inconsistent GPS tracks or timestamps, as well as event ID anomalies, highlighted potential manipulation or malicious intent. The inclusion of user badges, exercise logs and sleep log entry data provided insights into why attackers might target such data for profiling or exploitation. By analyzing the purpose behind anomalous device activities and their potential value to attackers, the framework offered deeper insights into the strategic importance of these digital attributes in cyberforensics investigations.

The construction of questions for open source intelligence (OSINT) data aligns its insights with the attributes extracted from wearable devices, enabling comprehensive incident reconstruction and enhancing cybersecurity investigations (see Table 2). The primary objective of these questions is to systematically address the 5W framework while establishing clear correlations with the digital attributes from wearable devices such as timestamps, GPS tracks, exercise logs, sleep log entries and user badges. This approach ensures a holistic understanding of incidents by leveraging both wearable device data and OSINT sources to provide actionable insights. For example, in the Who category, the questions are designed to identify individuals, entities or groups mentioned in the OSINT sources which could be linked to the incident or the recorded activity of the device. These questions are correlated with the attributes of the wearable device, such as the user ID, device info and device pairing status, to validate the legitimacy of interactions or flag suspicious behavior. This alignment allows for the identification of potential threat actors or unauthorized device interactions while evaluating their impact on the incident under investigation.

In the What category, OSINT questions focus on identifying significant events, trends or discussions related to the device's location or recorded behavior. For example, if a device's GPS tracks indicate its presence in a specific area, then OSINT questions could probe for reported incidents (e.g., thefts or protests) during the corresponding timeframe. These findings are then correlated with wearable device attributes such as the event ID, exercise logs and pairing status to assess whether the device's activity aligns with or deviates from legitimate behavior. By integrating data from OSINT and wearable devices, the framework can reconstruct the sequence of events with greater accuracy, ensuring that any malicious activity is flagged for further analysis.

The When category emphasizes temporal alignment between wearable device data and OSINT findings. Questions in this category aim to identify the timeline of events reported in OSINT sources and correlate them with timestamps, GPS activations and activity logs from wearable devices. For example, if OSINT sources report a vandalism protest at a specific time, then the framework compares this timestamp with the device's recorded activity to validate the device's involvement or rule out any connection. Dependencies between attributes in this category, such as timestamps, sleep log entries and their relationships with where and what, provide a structured view of the temporal patterns and their broader context.

Table 2. Questions for the synthesis of OSINT data.

5W Category	Questions for GenAI Model
Who	• Who were the key individuals or entities mentioned in reports of events (e.g., suspects and witnesses)? • Who are the potential threat actors associated with incidents near the device's location?
What	• What significant events were reported in the locations corresponding to the device's activity? • What types of online discussions or social media trends align with the recorded timestamps and locations?
When	• When were the reported events documented in public sources, and how do they correlate with the device's data? • When did related incidents occur in the broader geographic area?
Where	• Where did the reported events take place, and how do they align with the device's GPS tracks? • Where were potential threat actors or relevant individuals last seen, based on OSINT sources?
Why	• Why might the reported events be relevant to the device's recorded behavior or location? • Why do OSINT data suggest links between recorded incidents and broader malicious activities?

In the Where category, OSINT questions are designed to identify the locations of reported incidents and compare them with the device's GPS tracks, location data and pairing logs. This spatial correlation ensures that any recorded activity from the wearable device is evaluated against credible reports of incidents in the same geographic area. For instance, if OSINT sources document a reported theft at a particular location, then the framework uses the device's location attributes to determine whether its presence aligns with the event or raises suspicion. Dependencies between GPS tracks, location data and the pairing status enhance the precision of spatial alignment, allowing for a nuanced understanding of device behavior.

The Why category probes the motivations or potential implications behind observed incidents or behaviors. OSINT questions in this category aim to uncover the context or value of specific activities, such as why attackers might target particular user data or why deviations in device behavior might suggest malicious intent. These findings are then correlated with wearable device attributes such as the event ID, exercise logs, and user badges to provide a comprehensive understanding of the incident's context. Dependencies in this category, such as those between the device pairing status, user badges and temporal and spatial factors, help refine the understanding of intent and context.

By integrating these OSINT-driven questions with digital attributes from wearable devices, the framework facilitates precise threat detection, robust incident analysis and informed decision making. The structured evaluation of dependencies between wearable device data and OSINT insights ensures that correlations are systematically examined, providing CISOs with actionable insights and a comprehensive understanding of complex incidents. This approach enhances the accuracy of incident reconstruction and supports the development of targeted mitigation strategies to address emerging cybersecurity threats. Through the integration of wearable device data and OSINT, the framework sets a new standard for cyberforensics, enabling organizations to achieve greater resilience and preparedness in the face of evolving threats.

4.2. Experimental Validation with Public Datasets

To validate the proposed GenAI-assisted framework, we tested it using publicly available wearable device datasets [35]. The experimental scenario involved advertising, pairing and data exchange (specifically heart rate information) between a Garmin Vivoactive 4 smartwatch and a Samsung Galaxy S20 FE smartphone, followed by disconnecting. The digital attributes which were identified by GenAI were as follows.

Device Info:

- Wearable device: Garmin Vivoactive 4 (Bluetooth address: 14:13:0B:01:92);
- Master device: Samsung Galaxy S20 FE (Bluetooth address: 34:82:C5:37:DC:48).

Software/Hardware version:

- Recording device model: USRP X310 (software-defined radio); Daughterboard CBX-120; UHD Version 4.1.0.5-3;
- Wearable device model: Garmin Vivoactive 4; Bluetooth version 5.0; Android app Connect (version: 4.70);
- Master device model: Samsung Galaxy S20 FE; Bluetooth version 5.0.

Length:

- Recording duration: 16.986 s;
- Timeline description: enabling Bluetooth on smartphone = 1.307 s; disconnected duration = 14.98 s.

Protocol:

- Bluetooth communication: Bluetooth version 5.0 was used between the smartwatch and the smartphone.

Timestamp:

- Recording date: 21 November 2023;
- Recording location: EDI.

The initial 5W-driven report created by GenAI aimed to consolidate GPS data, timestamps and device information to assist in a cyberforensic investigation. The analysis provided context for identifying user behavior patterns, validating legitimate activity and recognizing anomalies which could indicate malicious actions:

- The Garmin Vivoactive 4 recorded the user's location in Edinburgh, Scotland, specifically in the city center area, near Princes Street. Princes Street is a well-known street in the city, often frequented by residents and tourists. (Remarks: This location information may be useful for corroborating user activity within Edinburgh's city center, especially in identifying any deviations from typical routes or verifying known events during the given timestamp).
- The Samsung Galaxy S20 FE, which serves as the master device, recorded GPS data which placed the user in Edinburgh, Scotland, specifically near Queen Street. Queen Street is within the central business district, which implies that the user was in a commercial area. (Remarks: These GPS data are significant as they tie the user's presence to a location in the commercial hub, which could have implications for activity verification, business interactions or identifying potential exposure to specific threats).
- The GPS data from the Google Pixel Watch indicated the user's presence near Holyrood Park, located in Edinburgh, Scotland. The data points specifically pointed to the Holyrood Road area, which is popular for outdoor activities and recreational use. (Remarks: This information is crucial for verifying user fitness activities, analyzing movement patterns and identifying any unusual activities that may not align with the user's regular behavior).

After the correlation of the initial 5W-driven report with the input of OSINT sources, the report and incident reconstruction were updated (Table 3).

Table 3. Event details summary.

5W Category	Results for Wearable Device 1	Results for Wearable Device 2
Who (device)	Garmin Vivoactive 4	Samsung Galaxy S20 FE
Where (location)	Princes Street Gardens	Princes Street Gardens
When (time)	19 January 2022	12 September 2024
What (event)	Man admits planting "bomb"; in Edinburgh's Princes Street Gardens	Protest involving vandalism at Barclays bank
Public source	[36]	[37]

5. Discussion and Limitations

The proposed GenAI-assisted framework offers significant potential in cyberforensics and strategic cyber resilience, particularly in addressing the complexities of modern cybersecurity challenges. By integrating generative AI into cyberforensics, the framework enhances the ability to cross-layer evidence from both the network and the application domains, enabling a comprehensive understanding of incidents. This includes leveraging wearable device data and open source intelligence (OSINT) to form a detailed 5W (who, what, when, where and why) analysis. This approach supports CISOs in identifying malicious activities, building attacker profiles, and generating contextual insights for better decision making. By automating the analysis of large datasets and providing dynamic incident scoring, GenAI can also optimize threat detection and incident response, improving resource allocation and preparedness.

5.1. Infrastructure and Performance Limitations

To successfully integrate GenAI into cyberforensics, it is essential to clearly comprehend and confront its intrinsic limits. Generative AI models are significantly dependent on processing power and computational resources, with their deployment potentially hindered by issues such as network latency, processing delays and environmental computational constraints. Latency in cloud-based GenAI models may hinder real-time issue identification and response, adversely impacting the speed and efficacy of cybersecurity operations. Furthermore, implementing GenAI locally or in edge contexts, like wearable devices or edge servers, may result in computational limitations due to the restricted processing power, memory and energy resources inherent in these settings. This requires meticulous evaluation of the infrastructure utilized by GenAI—be it cloud, edge or hybrid—to successfully balance performance and operational limitations. Future research should concentrate on evaluating these constraints in particular contexts and investigating optimization strategies, such as streamlined AI models or effective inference approaches, to alleviate these challenges and guarantee the dependable incorporation of GenAI into cybersecurity frameworks.

5.2. Data Accuracy and Operational Concerns

Despite the possibilities, the proposed GenAI-assisted framework has limitations. One of the main concerns is the dependency on accurate and vast datasets for GenAI to perform effectively. If training data are incomplete or biased, then the system can produce inaccurate or misleading results, particularly when reconstructing incidents from partial data. In this case, CISOs must continuously supervise the obtained results and the reliability assessment of those results. Furthermore, the framework's reliance on wearable device data poses privacy risks, as collecting and analyzing such data could raise concerns regarding personal data protection. Another challenge is that the integration of OSINT introduces potential vulnerabilities if the sources are unreliable or manipulated, leading to false intelligence, including GenAI hallucinations (such as fabricated or misleading results, including references to nonexistent facts). Indeed, the phenomenon of hallucinations is the most critical problem for GenAIs because it erodes the trust of end users, prevents adoption in diverse fields, and raises safety and privacy concerns [38–40].

Furthermore, the integration of GenAI into SOCs presents operational challenges, including model explainability, regulatory constraints and computational resource requirements. While the framework enhances threat prioritization and forensic automation, SOC analysts must validate GenAI-generated insights to mitigate risks associated with false positives or generative AI hallucinations. Future research should explore optimizing GenAI interpretability for security teams, ensuring compliance with industry standards and improving adversarial resistance in AI-assisted forensic models.

Since some CISO investigations can lead to legal proceedings, inaccuracies in GenAI outputs could undermine legal outcomes or infringe on human rights. The increasing use of GenAI in legal proceedings, along with its potential hallucinations, has led to guidelines for responsible implementation [41]. However, addressing and mitigating the inherent risk of hallucination is an ongoing challenge in the development and deployment of GenAIs, requiring not only ethical guidelines but careful monitoring and continuous refinement of their algorithms, training data and prompts [42–44].

5.3. Practical Implementation

To implement the proposed GenAI-assisted cyberforensics framework within an organization's existing security infrastructure, organizations should first assess their current security operations center (SOC) architecture and identify integration points with Security Information and Event Management (SIEM), Security Orchestration, Automation and Response (SOAR) and Threat Intelligence Platforms (TIPs). The framework should be deployed in a cloud, on-premises or hybrid environment based on security and compliance requirements. Organizations need to establish automated data ingestion pipelines to collect and correlate logs from wearable devices, network traffic and OSINT sources, ensuring real-time monitoring and cross-layer analysis. Security analysts should receive training on interpreting GenAI-assisted forensic reports, incident scoring and behavioral anomaly detection to enhance investigation efficiency. To address regulatory concerns, companies must implement explainable AI (XAI) methods and ensure compliance with GDPR, NIST and ISO 27001 standards [45] when handling personal and forensic data. Continuous model fine-tuning and adversarial testing should be performed to adapt to evolving threats and minimize AI biases or false positives. Finally, organizations should establish a feedback loop between SOC analysts and the GenAI system, allowing iterative improvements and increased trust in AI-driven security insights. By following these steps, organizations can integrate the GenAI-assisted framework into their security operations, improving threat detection, incident response automation and overall cyber resilience.

6. Conclusions and Future Work

The findings of this study offer a transformative approach to enhancing cyberforensics and strategic cyber resilience. By integrating cross-layered digital attributes from wearable devices and open source intelligence, it provides a more comprehensive analysis of cyber incidents, enabling CISOs to detect, assess and respond to threats with greater accuracy. By structuring incident analysis around the 5W approach, the GenAI-assisted framework enhances cybersecurity decision making through automated data synthesis and incident scoring.

While the framework strengthens security practices and enhances resilience in critical infrastructures, several challenges remain: (1) data privacy risks associated with analyzing personal information from wearable devices, which may raise legal and ethical concerns, (2) accuracy limitations due to GenAI hallucinations, potentially leading to misleading forensic conclusions, and (3) scalability constraints, as large-scale deployments may require optimized computing resources for real-time analysis.

For future work, efforts should focus on the integration of additional data sources, such as social media analytics or blockchain-based authentication, to improve the reliability of OSINT and provide a more holistic view of cyber incidents.

Author Contributions: Conceptualization, Š.G. and R.B.; methodology, Š.G. and R.B.; software, Š.G. and K.D.; validation, Š.G., R.B. and K.D.; formal analysis, R.D., I.V., Ž.N. and D.V.; investigation, Š.G.; resources, Š.G.; data curation, Š.G. and R.B.; writing—original draft preparation, Š.G. and R.B.; writing—review and editing, R.D., I.V., Ž.N., D.V., P.A., A.L., I.A. and N.G.; visualization, R.B.; supervision, Š.G.; project administration, Š.G.; funding acquisition, Š.G. All authors have read and agreed to the published version of the manuscript.

Funding: This paper was funded by the project "Research on Cyber Resilience Through Application of Generative Artificial Intelligence in Chief Information Security Officer Operations", which has received funding from the Research Council of Lithuania (LMTLT) (agreement No S-ITP-24-13).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this paper are available on request from the corresponding author. The incompleteness of the project prevents the data from being publicly available.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Ministry of National Defence. National Cyber Security Status Report. 2023. Available online: https://www.nksc.lt/doc/Nacionaline-kibernetinio-saugumo-ataskaita-2023.pdf (accessed on 28 December 2024).
2. ENISA. The European Union Agency for Cybersecurity. Artificial Intelligence and Cybersecurity Research. 2023. Available online: https://www.enisa.europa.eu/sites/default/files/publications/Artificial%20Intelligence%20and%20Cybersecurity%20Research.pdf (accessed on 8 January 2025).
3. European Union. Commission Welcomes Political Agreement on Artificial Intelligence Act. 2023. Available online: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6473 (accessed on 18 January 2025).
4. Kalodanis, K.; Rizomiliotis, P.; Anagnostopoulos, D. European Artificial Intelligence Act: An AI security approach. *Inf. Comput. Secur.* **2024**, *32*, 265–281.
5. Jemmett, D. CISO Workforce and Headcount 2023 Report. 2023. Available online: https://www.ciso.inc/2023-ciso-report/ (accessed on 18 January 2025).
6. Huang, K.; Ponnapalli, J.; Tantsura, J.; Shin, K.T. Navigating the GenAI Security Landscape. In *Generative AI Security: Theories and Practices*; Springer: Berlin/Heidelberg, Germany, 2024; pp. 31–58.
7. Prasad, S.G.; Sharmila, V.C.; Badrinarayanan, M. Role of artificial intelligence based chat generative pre-trained transformer (chatgpt) in cyber security. In Proceedings of the 2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC), Salem, India, 4–6 May 2023; IEEE: Piscataway, NJ, USA, 2023; pp. 107–114.
8. Mitra, R.; Schwieger, D.; Roy, I. Educating the Next Generation of CSOs: An Exercise in Conversational Role Play with ChatGPT. In Proceedings of the ISCAP Conference ISSN, Albuquerque, NM, USA, 1–4 November 2023; Volume 2473, p. 4901.
9. Dhoni, P. Unleashing the potential: Overcoming hurdles and embracing generative AI in IT workplaces: Advantages, guidelines, and policies. *TechRxiv* **2023**. [CrossRef]
10. Yigit, Y.; Buchanan, W.; Tehrani, M.; Maglaras, L. Review of Generative AI Methods in Cybersecurity. *arXiv* **2024**, arXiv:2403.08701.
11. ISC2. ISC2 Spotlight: Modernizing Security Operations. 2023. Available online: https://www.isc2.org/Insights/2023/10/ISC2-Spotlight-Modernizing-Security-Operations (accessed on 18 January 2025).

12. MacDermott, A.; Lea, S.; Iqbal, F.; Idowu, I.; Shah, B. Forensic analysis of wearable devices: Fitbit, Garmin and HETP Watches. In Proceedings of the 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Canary Islands, Spain, 24–26 June 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–6.
13. Zhang, Z.; Al Hamadi, H.; Damiani, E.; Yeun, C.Y.; Taher, F. Explainable artificial intelligence applications in cyber security: State-of-the-art in research. *IEEE Access* **2022**, *10*, 93104–93139. [CrossRef]
14. Henriques, J.; Caldeira, F.; Cruz, T.; Simões, P. A survey on forensics and compliance auditing for critical infrastructure protection. *IEEE Access* **2024**, *12*, 2409–2444. [CrossRef]
15. Ministry of National Defence. National Cyber Security Strategy. 2022. Available online: https://kam.lt/wp-content/uploads/2022/03/nacionaline-kibernetinio-saugumo-strategija.pdf (accessed on 11 January 2025).
16. Iturbe, E.; Rios, E.; Rego, A.; Toledo, N. Artificial Intelligence for next generation cybersecurity: The AI4CYBER framework. In Proceedings of the 18th International Conference on Availability, Reliability and Security, Benevento, Italy, 29 August–1 September 2023; pp. 1–8.
17. Preuveneers, D.; Joosen, W. An Ontology-Based Cybersecurity Framework for AI-Enabled Systems and Applications. *Future Internet* **2024**, *16*, 69. [CrossRef]
18. Bagirovs, E.; Provodin, G.; Sipola, T.; Hautamäki, J. Applications of Post-quantum Cryptography. *arXiv* **2024**, arXiv:2406.13258. [CrossRef]
19. Bountakas, P.; Fysarakis, K.; Kyriakakis, T.; Karafotis, P.; Aristeidis, S.; Tasouli, M.; Alcaraz, C.; Alexandris, G.; Andronikou, V.; Koutsouri, T.; et al. SYNAPSE—An Integrated Cyber Security Risk & Resilience Management Platform, with Holistic Situational Awareness, Incident Response & Preparedness Capabilities: SYNAPSE. In Proceedings of the 19th International Conference on Availability, Reliability and Security, Vienna, Austria, 30 July–2 August 2024; pp. 1–10.
20. European Union. A European Cyber Resilience Framework with Artificial Intelligence-Assisted Orchestration & Automation for Business Continuity, Incident Response & Information Exchange. 2022. Available online: https://cordis.europa.eu/project/id/101070586 (accessed on 11 January 2025).
21. Rastogi, N.; Dhanuka, D.; Saxena, A.; Mairal, P.; Nguyen, L. Survey Perspective: The Role of Explainable AI in Threat Intelligence. *arXiv* **2025**, arXiv:2503.02065.
22. Abusitta, A.; Li, M.Q.; Fung, B.C. Survey on Explainable AI: Techniques, challenges and open issues. *Expert Syst. Appl.* **2024**, *255*, 124710.
23. Capuano, N.; Fenza, G.; Loia, V.; Stanzione, C. Explainable artificial intelligence in cybersecurity: A survey. *IEEE Access* **2022**, *10*, 93575–93600.
24. Qureshi, S.U.; He, J.; Tunio, S.; Zhu, N.; Nazir, A.; Wajahat, A.; Ullah, F.; Wadud, A. Systematic review of deep learning solutions for malware detection and forensic analysis in IoT. *J. King Saud Univ.-Comput. Inf. Sci.* **2024**, *36*, 102164.
25. Ahmed, A.A.; Farhan, K.; Jabbar, W.A.; Al-Othmani, A.; Abdulrahman, A.G. IoT forensics: Current perspectives and future directions. *Sensors* **2024**, *24*, 5210. [CrossRef] [PubMed]
26. Rodrigues, F.B.; Giozza, W.F.; de Oliveira Albuquerque, R.; Villalba, L.J.G. Natural language processing applied to forensics information extraction with transformers and graph visualization. *IEEE Trans. Comput. Soc. Syst.* **2022**, *11*, 4727–4743. [CrossRef]
27. Odom, N.R.; Lindmar, J.M.; Hirt, J.; Brunty, J. Forensic inspection of sensitive user data and artifacts from smartwatch wearable devices. *J. Forensic Sci.* **2019**, *64*, 1673–1686.
28. Yoon, Y.H.; Karabiyik, U. Forensic analysis of fitbit versa 2 data on android. *Electronics* **2020**, *9*, 1431. [CrossRef]
29. Mishra, P. Secured Novel Lightweight IoT End Device Architecture using Confidentiality, Integrity, Authenticity & Availability based tight security approach. *Turk. J. Comput. Math. Educ. (TURCOMAT)* **2021**, *12*, 6768–6778.
30. Zhou, H. Comparison of Encryption Algorithms for Wearable Devices in IoT Systems. *Eng. Adv.* **2023**, *3*, 144–148.
31. Baucas, M.J.; Spachos, P.; Plataniotis, K.N. Federated learning and blockchain-enabled fog-IoT platform for wearables in predictive healthcare. *IEEE Trans. Comput. Soc. Syst.* **2023**, *10*, 1732–1741.
32. Santosa, G.B.; Budiyanto, S. New design of lightweight authentication protocol in wearable technology. *TELKOMNIKA (Telecommun. Comput. Electron. Control)* **2019**, *17*, 561–572.
33. Yu, S.; Park, Y. Robust and Efficient Authentication and Group–Proof Scheme Using Physical Unclonable Functions for Wearable Computing. *Sensors* **2023**, *23*, 5747. [CrossRef]
34. NIST; Aroms, E. *NIST Special Publication 800-86 Guide to Integrating Forensic Techniques into Incident Response*; NIST: Gaithersburg, MD, USA, 2012.
35. EDI Riga. Wearable_Device_Dataset. 2024. Available online: https://github.com/edi-riga/Wearable_device_dataset (accessed on 11 January 2025).
36. BBC. Man Admits Planting 'Bomb' in Edinburgh's Princes Street Gardens. 2022. Available online: https://www.bbc.com/news/uk-scotland-edinburgh-east-fife-60059070 (accessed on 19 January 2025).
37. BBC. Barclays Branches Across UK Targeted by Protesters. 2024. Available online: https://www.bbc.com/news/articles/c1rrzp1qwp1o (accessed on 19 January 2025).

38. Chrysostomou, G.; Zhao, Z.; Williams, M.; Aletras, N. Investigating hallucinations in pruned large language models for abstractive summarization. *Trans. Assoc. Comput. Linguist.* **2024**, *12*, 1163–1181.
39. Ji, Z.; Lee, N.; Frieske, R.; Yu, T.; Su, D.; Xu, Y.; Ishii, E.; Bang, Y.J.; Madotto, A.; Fung, P. Survey of hallucination in natural language generation. *ACM Comput. Surv.* **2023**, *55*, 1–38.
40. Farquhar, S.; Kossen, J.; Kuhn, L.; Gal, Y. Detecting hallucinations in large language models using semantic entropy. *Nature* **2024**, *630*, 625–630. [PubMed]
41. Grossman, M.R.; Grimm, P.W.; Brown, D.G. Is disclosure and certification of the use of generative AI really necessary? *Judicature* **2023**, *107*, 68–77.
42. Yamin, M.M.; Hashmi, E.; Ullah, M.; Katt, B. Applications of llms for generating cyber security exercise scenarios. *Preprint* **2024**, *12*, 143806–143822.
43. Patil, R.; Heston, T.F.; Bhuse, V. Prompt engineering in healthcare. *Electronics* **2024**, *13*, 2961. [CrossRef]
44. Olla, P.; Elliott, L.; Abumeeiz, M.; Mihelich, K.; Olson, J. Promptology: Enhancing Human–AI Interaction in Large Language Models. *Information* **2024**, *15*, 634. [CrossRef]
45. International Organization for Standardization. ISO/IEC 27001:2022—Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements. 2022. Available online: https://www.iso.org/standard/27001 (accessed on 15 January 2025).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.