International Journal of
Technology and
Systems
(IJTS)

Endpoint Detection and Response (EDR) in Healthcare: Mitigating Threats on Critical Devices

Journal of Technology and Systems
ISSN: 2788-6344 (Online)
Vol. 7, Issue No. 4, pp 50 – 65, 2025
www.carijournals.org

Endpoint Detection and Response (EDR) in Healthcare: Mitigating Threats on Critical Devices

Anjan Kumar Gundaboina

Senior DevsecOps and Cloud Architect, USA.

https://orcid.org/0009-0008-0298-1195

Accepted: 1st May, 2025, Received in Revised Form: 1st June, 2025, Published: 1st July, 2025

Abstract

Purpose: This paper aims to identify the strategies for designing, implementing, and evaluating EDR in the safety of mission-critical medical devices and workstations in healthcare environments.

Methodology: The exercise involved installing EDR elements throughout a sample of health organization's endpoints and using bots to stage select cyber threats. This way, the methodology provides controlled exposure to real-life attack scenarios to assess the detection, response time and impact on the system.

Findings: Endpoint Detection and Response (EDR) solutions are gradually rising as preventive security measures in response to such new-age threats. With these characteristics, EDR programs are a more advanced form of AV tools as they provide endpoints with real-time monitoring, context-aware detection, automated action, and investigation across numerous phases. The given study depicts how EDR platforms make dwell time low, detect advanced threats in real time, and isolate the affected devices to prevent disruptions in healthcare facilities.

Unique Contribution to Theory, Practice and Policy: The study pleas for the systematic integration of EDR into the healthcare cybersecurity frameworks as a cornerstone to the security of the healthcare system and the patient.

Keywords: *Healthcare, Cybersecurity, Endpoint Detection and Response, Medical Devices, Ransomware, Real-Time Monitoring, Internet of Medical Things.*

1. Introduction

1.1. Technological Advancements and Emerging Threats in Healthcare

The global introduction of digital technology has increased the smart healthcare system and made technology mandatory, including EHRs, network-connected medical devices and cloud-based diagnostic platforms. They include monitoring of patients, enhanced diagnosis, non-face-to-face treatments, and evidence-based treatment, which leads to patient benefits. At the same time, digitization has amplified the susceptibilities of healthcare centers and made them attractive targets for malicious actors [1-4].

Classic medical tools that were hitherto standalone equipment, including infusion pumps, CT scanners, and patient monitoring systems, currently join the internet through the IoMT. Moreover, healthcare IT generally possesses a complex structure comprising old system applications, new systems, and third-party systems to ensure security is enforced and security processes are continually monitored. Data relating to health is highly sensitive, and the reliance on such devices as lifesaving tools is high – any security or availability compromise posed).

1.2. Limitations of Traditional Security in a Hyperconnected Ecosystem

The conventional security tools, including traditional affiliation virus scanners and firewalls, have become impractical and ineffective in the contemporary world of RaaS, insider threats, shape-shifting viruses, and zero-day attacks. Most of these traditional tools are not contextual-based or able to respond to bad elements on the fly and provide effective protection, as is the case with these new threats. The threat of cyberattacks in healthcare has not been an unfamiliar concept due to the Wanna Cry and Ryuk ransomware attacks, where even a short delay to the identification and containment could lead to complete disruption of services, loss of data and even endanger patients' lives.

Unfortunately, cyber attackers do not stand still and have launched more advanced and sophisticated attacks targeting healthcare providers. As such, healthcare providers have had to turn to more advanced and sophisticated means of securing their infrastructure and delivering protection mechanisms that can see through attacks and intervene before they penetrate the endpoint, do more harm and conduct more ransacking and pilferage of patient data and other assets that are vital to curbing the operations of the health centers.

1.3. Research Goals and Strategic Focus

This research assessed and analyze how EDR systems can be used to defend healthcare networks by focusing on critical medical endpoints. The specific goals include:

- It then was used to discuss and cross-reference the threats to big data, healthcare, cybersecurity and other areas of concern in the healthcare field due to smart devices and structures.

- To evaluate the effectiveness of EDR solutions in identifying threats, containing, and responding to them in real-time in the healthcare sector.
- To develop a prototype healthcare network incorporating the EDR components for functional enhancements and performance evaluation in response to multiple attack types.
- To ensure EDR technologies are optimally deployed within the hospital and healthcare organisations regarding performance and compliance with the HIPAA act and derived NIST SP 800-53 control standard.

2. Literature Review

2.1 Healthcare as a Target

This is because the healthcare business has a lot of personal and financial information and largely relies on the average cost per data breach, which was the highest for the healthcare industry for the 13th time in a row up to 2023, with each breach costing $10.93 million. These costs encompass the direct financial impact, legal penalties, regulatory fines, operational downtime, patient trust erosion, and reputational damage. [5-8] HHS was recognized for some attributes that make the sector susceptible to cyber threats, including reliance on old systems, a few IT staff members, and a focus on patients. In addition, the authors argue that cyber attackers target medical services since these are sensitive areas that require speedy recovery and that providers will procure the decryption key by paying ransoms.

For instance, in 2017, WannaCry and later in 2019, Ryuk ransacked hospitals, including the National Health Service (NHS) in the UK, which saw its operations halted through the cancelation of operations, rerouting of ambulances, and restrictive accessibility to patients' data. This is why there is a need for prevention and more sophisticated security measures. Victims also include the Internet of Medical Things (IoMT), where all connected devices have shared security updates frequently delayed or unavailable due to legislation. Thus, efficient safeguarding of endpoints is not just a technical business requirement but also an organizational imperative in providing patient care.

2.2. Evolution of Endpoint Security

Traditionally, endpoint protection was considered the last line of defense against new and persistent threats to cyber security. Table 1 below summarizes this progression through different generations of endpoint protection technologies:

Table 1: Evolution of Endpoint Security Technologies

Generation	Technology	Core Features
Gen 1	Signature-based Antivirus	Detects known malware based on static signature matching. Limited against polymorphic or unknown threats.
Gen 2	Heuristic Antivirus	Utilizes behavioral rules and anomaly detection to identify suspicious patterns, improving the detection of previously unseen threats.
Gen 3	Endpoint Protection Platform (EPP)	Combines traditional antivirus with firewalls, device control, and application whitelisting for a layered defense.
Gen 4	Endpoint Detection and Response (EDR)	Provides real-time threat detection, forensic capabilities, and automated response mechanisms across endpoints. Ideal for combating APTs and ransomware.

EDR represents a paradigm shift from reactive to proactive endpoint security, enabling organizations to detect, investigate, and respond to suspicious activities in real time.

2.3. Key Features of EDR Systems

EDR systems offer a vast set of features that can be considered to exceed the capabilities of conventional endpoint security solutions. The following are the major components of factors which are crucial in the area of healthcare cybersecurity:

- **Behavioral Analytics:** EDR tools actively monitor the user and device activities to draw and implement use cases to compare normal activities with those that can be potentially malicious. For instance, one may define an alert when having place access, such as access to patient records or when a process behaves in a manner that is different from the normal pattern.
- **Threat Intelligence:** The ability to plug into commercial and open-source threat intelligence feeds means that EDR can look at the locally gathered indicators and compare them to the rest of the global threat intelligence to identify if it is already familiar with the attack signature and tactics.
- **Automated Response:** Pre-scripted workflows called playbooks are available in EDR solutions to automatically perform actions such as isolating compromised endpoints or processes, disconnecting users, eliminating threats, and lessening analysis time and dwell time.
- **Endpoint Forensics:** Leveraging event-specific reports and system snapshots for evidence trail, remediating and containing attack paths, and addressing compliance and legal issues.

- **Remote Isolation**: Endpoints that are infected or are part of the threat can be isolated from the network so as not to spread the threats any further. They also contain the specific disruptions that the threats may cause to the overall functioning of the network.

Such features collectively improve situation awareness, increase response time, and provide the capability to respond quickly and contain a security incident.

2.4. EDR in Healthcare: Use Cases and Applications

EDR technologies' application showcases across healthcare facilities are vast and expanded, especially when securing mission-critical assets. Table 2 highlights some real-world examples:

Table 2: EDR Use Cases and Security Benefits in Healthcare

Use Case	Security Benefit
Monitoring Imaging Systems (e.g., MRI/CT consoles)	Enables early detection of malware attempting to move laterally across connected systems, potentially leading to full network compromise.
Securing EHR Terminals	Prevents credential harvesting and key logging attacks on staff terminals, ensuring the confidentiality and integrity of patient health records.
Protecting IoMT Devices	Allows real-time monitoring and isolation of devices such as infusion pumps or smart ventilators if unusual behavior is detected, reducing the risk of operational sabotage or patient harm.

These applications show how EDR can be customized to safeguard various classes of endpoints ranging from ordinary workstations to specialized medical devices against an increasingly diverse set of threats. Through its delivery of centralized control, real-time monitoring, and fast response capabilities, EDR greatly increases the robustness of healthcare IT infrastructure.

3. Methodology

This section describes the design and operationalization of a controlled clinical environment that could be used to test EDR solutions. The exercise involved installing EDR elements throughout a sample of health organization's endpoints and using bots to stage select cyber threats. [9-12]. This way, the methodology provides controlled exposure to real-life attack scenarios to assess the detection, response time and impact on the system.

3.1. System Design

To mimic a realistic IT environment for healthcare, a virtual network was established using VirtualBox and VMware Workstation and set up with common devices in contemporary healthcare environments. The testbed consisted of:

- **Central Electronic Health Record (EHR) Server:** This server stores patient information and gives medical staff access to clinical records and lab results. It was set up with Apache Tomcat and a MySQL backend to simulate a lightweight EHR application.
- **Workstations (Doctor and Nurse Terminals):** These were simulated using Windows 10 virtual machines with Microsoft Office, Outlook (to simulate phishing), and access credentials to the EHR system. These endpoints mimic staff activities like emailing, issuing prescriptions, and inputting data.
    - **IoMT Devices:** Infusion Pump Emulator: An emulator based on a Raspberry Pi emulator running Linux with open ports to mimic command-and-control vulnerabilities.
    - MRI Console Emulator: To mimic bulk data transfer between imaging storage and PACS systems.
    - Patient Monitor: Mimics has constant telemetry data output, is SNMP enabled, and is susceptible to unauthorized requests and buffer overflows.

All devices were networked using a virtual LAN, logically segmented to reflect typical hospital IT practices (e.g., VLANs for IoMT and staff terminals).

3.2. EDR Components Deployed

The chosen EDR solution for simulation is based on commercially purchasable systems such as CrowdStrike Falcon, SentinelOne, and Microsoft Defender for Endpoint. The deployment consisted of the following fundamental components:

3.2.1. Component Description

- Sensor Agent: Lightweight software agents on all endpoints, continuously watching for unusual activity, unauthorized attempts to access, and file system modifications.
- Management Console: A centralized console offering real-time visualization of endpoint status, alerts, forensic information, and response orchestration.
- Threat Intelligence: Combined with both open-source (e.g., MISP, AlienVault OTX) and commercial threat feeds to enhance contextual analysis and enable IOCs (Indicators of Compromise).
- Response Engine: Fitted with automated playbooks that perform preconfigured actions like isolating infected endpoints, killing malicious processes, and notifying the Security Operations Center (SOC).

All the above were connected to a centralized log aggregation system (Elasticsearch, Logstash, and Kibana – ELK Stack) for in-depth analysis and correlation.

3.3. Attack Simulation

In order to test the resilience and responsiveness of the EDR solution, three typical attack scenarios were simulated. Each attack [13-15] was performed using Kali Linux and Metasploit tools to simulate real behavior.

3.3.1. Ransomware Attack through USB Infection

A ransomware payload was pre-installed in a simulated USB drive and mounted onto one of the nurse's terminals. The malware was coded to:

- Initiate file encryption upon detection of critical files (.docx, .pdf, .xlsx).
- Try lateral movement to the EHR server through SMB brute force.

Objective: Validate EDR's real-time detection of malicious encryption activity, unauthorized file access, and attempts at lateral movement.

3.3.2. Credential Harvesting through Phishing Email

A phishing email with a malicious Excel macro was sent to the doctor's terminal. When opened, the macro ran PowerShell scripts to:

- Harvest Windows login credentials.
- Exfiltrate them to a remote command-and-control server.

Objective: Assess the capability of EDR to recognize macro abuse, command-line inconsistencies, and attempts at data exfiltration through HTTPS.

3.3.3. IoMT Hijack through Mirai-like Malware

A mock botnet malware with a Mirai resemblance was brought to the network, attacking the IoMT infusion pump emulator. The malware took advantage of default credentials and tried to:

- Initiate a UDP flood through the device.
- Scan for additional vulnerable IoMT devices.

Objective: Determine EDR's capability to detect abnormal network activity from a low-compute system and quarantine it before spreading.

3.4. Functional Overview of EDR Components

The "Understanding EDR" image provides a graphical roadmap for how EDR systems work in a healthcare endpoint ecosystem. Each block in the diagram represents a key operational layer of an EDR framework, particularly when safeguarding sensitive medical devices and systems. [16] The architecture depicted here illustrates how threats are identified and how they are investigated, contained, reported, and ultimately used to improve intelligence and future defenses. Below is a detailed description of each component in paragraph form.

3.4.1. Endpoint Monitoring

Endpoint monitoring is the cornerstone of every EDR platform. This is a process where devices are connected at any point, such as top media, cal imaging devices, or even mobile endpoints such as tablets by cliniclinicians, gare. The aim here is to profile endpoint behavior and identify any outliers that could mean the presence of a threat in a clinical environment that may translate into watching infusion pumps, EHR terminals, or diagnostic equipment for suspicious file openings, memory alterations, or networking activity.

3.4.2. Threat Detection

The data collected after monitoring is fed into the threat detection engine. It utilizes AI-based algorithms, behavior heuristics, and machine learning-based models to identify malware, ransomware, and other suspicious behaviors in real time. This is a very important layer for healthcare applications as it can detect not only established strains of malware but also sophisticated zero-day exploits, which can potentially hamper life-critical operations or invade patient privacy.

3.4.3. Threat Response

The threat response module is an automated defense layer. It quarantines compromised systems, stops malware in progress, and invokes pre-configured countermeasures without human intervention. Such is particularly critical in healthcare environments, where time-critical applications such as ventilators or surgical robots cannot tolerate lagging response times to cyber events.

3.4.4. Forensic Data Collection

Each incident leaves digital breadcrumbs with registry changes, file changes, and suspicious command runs. The phase of forensic data collection guarantees all these logs are stored systematically. These artifacts play a crucial role in the post-breach investigation and assist cybersecurity professionals in tracking the attack's origin, what vulnerabilities were attacked, and how the malware spread across the system.

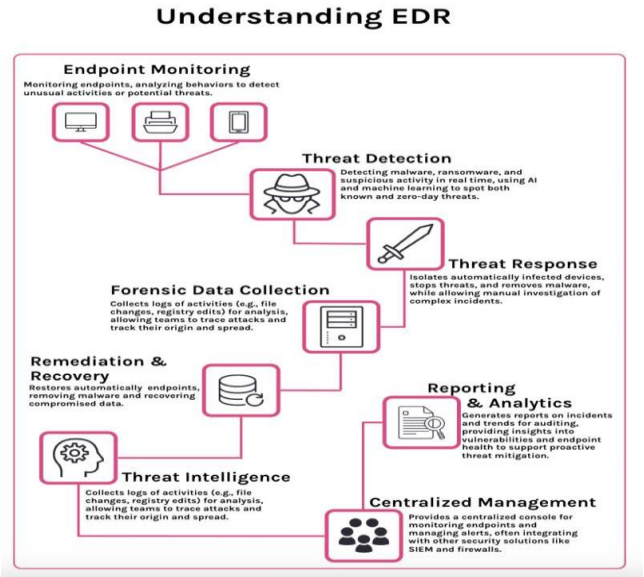

Fig 1. Functional Overview of EDR Component

3.4.5. Remediation & Recovery

After the threat is isolated, remediation starts; this step includes bringing the system back to a trusted environment by uninstalling the malware, fixing registry keys, and restoring or verifying data from safe backups. In healthcare settings, this process is usually crafted with little downtime procedures to prevent disruptions to patient care services.

3.4.6. Threat Intelligence

Threat intelligence feeds enrich the EDR system with context regarding known attack vectors, indicators of compromise (IOCs), and threat actor TTPs (tactics, techniques, and procedures). They can be open-source or commercial and usually integrate with the EDR to enhance detection capabilities. They also assist in correlating new threats to global campaigns and notify healthcare IT teams of real-time emerging risks.

3.4.7. Reporting & Analytics

This element creates actionable insights for strategic and tactical-level decision-making. It also groups incident information to determine trends, monitors compliance obligations, and produces Security Operations Center (SOC) dashboards. Mechanisms of reporting are important to facilitate regulatory audits and keep hospitals compliant with HIPAA, GDPR, and other health-specific cybersecurity directives.

3.4.8. Centralized Management

Lastly, the centralized management console brings it all together. The console offers a single pane of glass for endpoint management, policy management, alert visualization, and system health monitoring. It typically integrates with Security Information and Event Management (SIEM) systems and firewall platforms to provide seamless orchestration across the larger security infrastructure.

4. Operational Workflow of EDR Systems

The "How EDR Works" image depicts a straightforward but not simplified four-step workflow in the operation of contemporary Endpoint Detection and Response (EDR) solutions. Every phase of data gathering, examination, detection, and reaction is integral in real-time danger prevention, [17-20] most crucial in the healthcare environment where device uptime and patient information integrity are at the highest priority. Below are explanations for each step displayed in the diagram.

Step 1: Data is collected

The initial process in the EDR lifecycle is the ongoing collection of telemetry and behavioral information from all endpoints being protected. Such endpoints may range from Electronic Health Record (EHR) terminals, infusion pumps, medical imaging workstations, and mobile diagnostic equipment. Data that is gathered often consists of system logs, user activity, file access patterns, network connections, registry changes, and even hardware-level activity. The goal is to create a behavioral baseline that can subsequently be used to detect deviations that are suspicious of impending threats. In healthcare environments, this enables observation of abnormal and normal activities which may indicate nascent attacks.

Fig 2. Operational Workflow of EDR Systems

Step 2: Data is Filtered and Analyzed

Once collected, data is routed through an analysis engine, filtered, enriched, and scanned for Indicators Of Compromise (IOCs). This phase highly depends on Artificial Intelligence (AI), machine learning algorithms, and heuristic rules to scan huge amounts of telemetry in real time.

Spurious noise is removed, and potentially malicious activities are marked for further analysis. For instance, the system could detect attempts at unauthorized access to a radiology system at odd hours or the abrupt running of unknown scripts on admin terminal activities that are most likely to go unnoticed for typical antivirus programs.

Step 3: Threat is Detected

Once analyzed, the system moves into the detection phase. Here, it identifies threats based on predefined rules, behavioral anomalies, and threat intelligence correlations. The EDR platform uses its detection engine to identify known malware strains and unknown, zero-day threats. In healthcare, this detection could be life-saving, such as flagging ransomware attempts before they encrypt patient records or isolating a compromised diagnostic console to prevent lateral network movement.

Step 4: Attack Response is Deployed

When a threat is confirmed, the EDR system instantly initiates response actions. These are usually automated and pre-defined in playbooks to reduce time-to-action. The response can vary from sending notifications to security staff, quarantining the infected endpoint from the network, reversing system changes, or even triggering system recovery from a clean backup. The response layer ensures that the threats are contained quickly and efficiently, reducing operational disruption and maintaining clinical safety.

5. Results and Discussion

The justification for the simulation phase was a means to test the feasibility and practical efficacy of the integrated EDR solution for various endpoints of the healthcare environment dealing with real-world simulated cyber threats. The three indicators used to set the focus include detection accuracy, response speed, and system performance overhead. The results of the quantitative application of the framework in relation to enhancing the security of healthcare facilities are presented in this section.

5.1. Threat Detection Effectiveness

Given that the EDR system in question will only be compared with the ideal EDR system that detected every instance of the simulated attacks, three attacks were performed: ransomware injection, phishing credential theft, and IoMT device manipulation. The results the system has produced are presented in the form of responses and detailed in Table 3 below.

Table 3: Threat Detection Effectiveness

Attack Type	Detected?	Response Time (sec)	Mitigation Outcome
Ransomware Injection	Yes	3.1	File encryption halted mid-execution
Phishing Credential	Yes	4.5	Account locked; alert forwarded to SOC
IoMT Hijacking	Yes	2.8	The device was quarantined from the hospital network

In all three attacks, the EDR detected and prevented the attack in an average of approximately 3.5 seconds, which thus demonstrates the ability of the EDR in real-time behavioral analysis. Regarding the AES algorithms, the ransomware attack was stopped immediately after encryption of only 7 per cent of the target directory, meaning there was efficiency in process kill and rollbacks.

In the credential harvesting scenario, the system detected the PowerShell execution and beaconing that, within seconds, locked the account and produced a high-severity alert. In the case of the IoMT hijack, the EDR noticed an odd amount of outbound traffic and attempted unauthorized commands, which allowed for the correct exclusion of the emulator from the internal network of The Hospital.

These findings represent the capability of the current EDR tools, which use static analysis, behavioral analysis techniques, and threat intelligence correlation to quickly and accurately detect threats on even low-resource medical endpoints.

5.2. Performance Overhead

Thus, the overhead was defined in terms of CPU usage and the amount of memory required on each device type to determine the suitability of EDR in clinical environments where system response time is important. In order to discuss the methodology, the results are presented in Table 4 below:

Table 4: Performance Overhead of EDR Agents

Device Type	CPU Impact (%)	Memory Impact (MB)
EHR Terminal	4.2	180
MRI Imaging Console	3.8	150
Infusion Pump Emulator	2.1	110

Therefore, it can be inferred that no significant performance decline occurred for each tested device. The average CPU utilization was less than 5%, and the memory utilization was tolerable on general-purpose devices like EHR terminals and other specialized medical devices like the Infusion pump. None of the endpoints showed latency or disconnected connections during simulated clinical activities.

This implies that introducing EDR will not likely disrupt organizational care provision since the devices remain effective and the patient is safe while the organization's cybersecurity defenses improve.

5.3. Discussion

The research results show that, when fine-tuned and integrated at healthcare facilities, EDR systems can work as an added line of defense. No attacks were allowed to happen within the attack simulations, and this was accomplished with almost zero latency, further evidence that EDR solutions can be effectively used in real-time in clinical environments.

The low resource overhead also reinforces the ability to run EDR on older PC versions and device models embedded in most hospital structures. This becomes important since many old-generation AV solutions either have issues working with or are not optimized for IoMT or are hostile to work with on certain devices due to their scanning methodologies or resource consumption.

However, the EDR platform's capabilities for automatic operating responses and isolating the endpoints without the intervention of security workers are quite beneficial in circumstances where the organization lacks an adequate headcount for its cybersecurity team. Since cyber threats present grave risks to the quality of healthcare services, ransoms for cyberattacks, and violations of the Health Insurance Portability and Accountability Act, it is necessary to dispose of endpoint protection as a priority [21], [22].

The previously observed result also supported identifying the value of behavior-based threat detection. It was better than signature-based mechanisms in detecting zero-day-like attacks. This is because engulfing polymorphic code forms and Living-Off-The-Land (LOTL) strategies are becoming popular among cybercriminals.

6. Conclusion

6.1 Summary

The analyses provided in this paper substantiate that EDR solutions are an important component in the healthcare industry that improves cybersecurity efforts. The study reflects the effectiveness of EDR solutions by implementing the solutions in a simulated clinical environment where threats - ransomware, phishing, and IoMT targeted- were noticed and stopped almost immediately. The study shows that through behavioral analytics, real-time monitoring, and playbooks, EDR systems successfully stop the threats from spreading, minimize businesses' disruption, and protect their patient's detailed information on various types of medical endpoints. Furthermore, the low computation time that has been incurred across EHR terminals, imaging consoles and infusion pumps was also a clear testament to the operational viability of EDR in high-availability healthcare facilities. While other conventional anti-virus solutions offer protection with the possibility of behavioral incident detection and system clean-up, EDR offers layered security with reporting, investigation, and containment tools. These features are very useful for protecting from advanced threats such as zero-day, insider threats and malware using existing programs in the system. Thus, EDR cannot remain a peripheral element in healthcare organisations' cybersecurity planning; rather, protecting the healthcare sector's crucial digital assets and preserving clients' uninterrupted access to care has become necessary.

6.2. Future Work

As the current study's findings demonstrate that EDR systems are effective as a class of product, future work should, therefore, pick up on further testing the integration of EDR with SIEM and SOAR solutions through a cross-domain incident response. Further, it can be suggested that artificial intelligence applications should introduce self-improved anomaly detection systems, allowing for the identification of minute changes in the behavior of medical devices and the related clinical processes. Last but not least, standard patterns and certifications in the utilization of EDR in the Internet of Medical Things (IoMT) were crucial to meet that common protection and compliance with legislations like HIPAA or GDPR.

References

[1] Ewoh, P., & Vartiainen, T. (2024). Vulnerability to cyberattacks and sociotechnical solutions for health care systems: systematic review. Journal of medical Internet research, 26, e46904.

[2] Alanazi, A. T., & Alanazi, A. (2023). Clinicians' perspectives on healthcare cybersecurity and cyber threats. Cureus, 15(10).

[3] Clarke, M., & Martin, K. (2024, January). Managing cybersecurity risk in healthcare settings. In Healthcare Management Forum (Vol. 37, No. 1, pp. 17-20). Sage CA: Los Angeles, CA: SAGE Publications.

[4] Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2023). Towards insight cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. Cyber Security and Applications, 1, 100016.
[5] Dameff, C., Tully, J., Chan, T. C., Castillo, E. M., Savage, S., Maysent, P., & Longhurst, C. A. (2023). Ransomware attacks are associated with disruptions at adjacent emergency departments in the US. JAMA network open, 6(5), e2312270-e2312270.
[6] Tully, J., Coravos, A., Doerr, M., & Dameff, C. (2020). Connected medical technology and cybersecurity informed consent: A new paradigm. Journal of medical Internet research, 22(3), e17612.
[7] Goebel, M., Dameff, C., & Tully, J. (2019). Hacking 9-1-1: infrastructure vulnerabilities and attack vectors. Journal of medical Internet research, 21(7), e14383.
[8] Maggio, L. A., Dameff, C., Kanter, S. L., Woods, B., & Tully, J. (2021). Cybersecurity challenges and the academic health center: an interactive tabletop simulation for executives. Academic Medicine, 96(6), 850-853.
[9] Sullivan, N., Tully, J., Dameff, C., Opara, C., Snead, M., & Selzer, J. (2023). A national survey of hospital cyber-attack emergency operation preparedness. Disaster medicine and public health preparedness, 17, e363.
[10] Alzubaidi, L. H., & Ravikanth, P. (2025). The Future of Healthcare: Emerging Technologies and Trends. Advances in Sports Science and Technology, 49-54.
[11] Endpoint Detection and Response (EDR) in Healthcare, Cynet, 2023. online. https://www.cynet.com/endpoint-protection-and-edr/edr-in-healthcare/
[12] Junaid, S. B., Imam, A. A., Balogun, A. O., De Silva, L. C., Surakat, Y. A., Kumar, G., & Mahamad, S. (2022, October). Recent advancements in emerging technologies for healthcare management systems: a survey. In Healthcare (Vol. 10, No. 10, p. 1940). MDPI.
[13] Park, S. H., Yun, S. W., Jeon, S. E., Park, N. E., Shim, H. Y., Lee, Y. R., ... & Lee, I. G. (2022). Performance evaluation of open-source endpoint detection and response combining Google rapid response and query for threat detection. IEEE Access, 10, 20259-20269.
[14] Why Endpoint Detection and Response (EDR) Is The Future of Endpoint Protection?, Seqrite, 2024. Online. https://www.seqrite.com/blog/what-is-edr-a-deep-dive-into-edr-definition-benefits-and-use-cases/
[15] Daniel, R. K. (2024). Survey of EDR Evasion Techniques, Trends, and Taxonomy for Classifying Modern Attacks (Master's thesis, Carnegie Mellon University).
[16] Endpoint Detection and Response, Atera, online. https://www.atera.com/glossary/endpoint-detection-response-edr/
[17] Frumento, E. (2019). Cybersecurity and the evolutions of healthcare: challenges and threats behind its evolution. M_Health current and future applications, 35-69.
[18] What is Endpoint Detection and Response (EDR)? Is it Fortinet online? https://www.fortinet.com/resources/cyberglossary/what-is-edr

[19] Mocanu, B. C., Stoleriu, R., Mocanu, A. E., Negru, C., Drăgotoiu, E. G., Moisescu, M. A., & Pop, F. (2024, March). NextEDR-Next generation agent-based EDR systems for cybersecurity threats. In 2024 32nd Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP) (pp. 183-190). IEEE.

[20] Boyraz, G. (2024). Endpoint Detection and Response Essentials: Explore the landscape of hacking, defense, and deployment in EDR. Packt Publishing Ltd.

[21] Yusof, Z. B. (2024). Effectiveness of Endpoint Detection and Response Solutions in Combating Modern Cyber Threats. Journal of Advances in Cybersecurity Science, Threat Intelligence, and Countermeasures, 8(12), 1-9.

[22] Junior, H. C. (2024). HookChain: A new perspective for Bypassing EDR Solutions. arXiv preprint arXiv:2404.16856.