ENDPOINT DATA THREAT PROTECTION SOLUTIONS SYSTEM

Charleton Kiambuthi Ng’ang’a

Abigail Mathaiya Wahu

A proposal submitted to Zetech University for the partial fulfillment of the award of Bachelor of Business Information Technology

2024

Declaration

This proposal/research project is my original work and has not been presented for a diploma in any other colleges.

…… ……

Signature Date

This proposal/research project has been submitted for examination with my approval as college Supervisor.

…… ……

Signature Date

Abstract

The risk of data breaches and cyber threats has increased dramatically in today's constantly changing digital ecosystem due to the increased reliance on networked systems and endpoints, particularly for firms that lack strong security measures. Endpoints—computers, smartphones, and other hardware that is connected—are especially prone to becoming entry points for hackers to initiate assaults. The creation of an Endpoint Data Threat Protection Solutions System is described in this proposal, which aims to reduce risks by offering complete endpoint device protection via real-time threat detection and prevention. The study commences by scrutinizing the present condition of endpoint security, pinpointing vulnerabilities, and delving into the particular obstacles encountered by small and medium-sized organizations (SMEs) when it comes to network security.

Because they lack sophisticated security architecture and have limited resources, SMEs are frequently the target of cybercriminals. Businesses are more vulnerable to dangers like malware, ransomware, phishing attempts, and data theft as they grow and incorporate new technologies. Endpoint devices are the primary points of contact for users and sensitive data, thus keeping them secure is essential to upholding organizational integrity and safeguarding important data. Developing a customized endpoint security system that meets the unique requirements of enterprises is the primary goal of this research, with an emphasis on real-time threat detection, response, and prevention.

To identify and stop malicious activity at the endpoint level, the solution will make use of a mix of sophisticated machine learning algorithms, intrusion detection systems, and behavioral analytics. The system will be able to react swiftly to attacks by continually monitoring endpoint devices, reducing the possibility of data breaches and guaranteeing uninterrupted, safe corporate operations. This study will use a combination of qualitative and quantitative methods in its methodology. A thorough examination of the literature will be done in order to assess current frameworks and solutions related to endpoint security. Furthermore, surveys and interviews with cybersecurity and IT specialists will be undertaken to obtain information on the most urgent issues that companies are facing with endpoint security. This original data will assist in determining the gaps.

In order to assess how well the suggested system performs in identifying and averting different kinds of cyber threats, the research will also include testing it in a simulated setting. The efficacy of the system will be evaluated by measuring metrics including false positive rates, reaction times, and detection accuracy. The benefits and enhancements provided by the suggested system will be assessed by contrasting the outcomes with those of current endpoint security solutions. Major research findings should emphasize how crucial it is to approach endpoint security pro-actively, with an emphasis on automated threat response and real-time monitoring. Threat identification and mitigation will probably benefit greatly from the endpoint security system's integration of machine learning and behavioral analytics.

In conclusion, companies looking to protect their data and operations from cyber-attacks will have a reliable and scalable option with the Endpoint Data Threat Protection Solutions System. The technology will enable companies to improve their cybersecurity posture and ensure that they are able to adjust to the constantly shifting threat landscape by tackling the unique obstacles that SMEs encounter. It is anticipated that this solution's application will lessen data breaches and the monetary losses brought on by cyberattacks, eventually allowing companies to confidently concentrate on their main business operations.

Table of Contents

Acronyms

- **EDTPS:** Endpoint Data Threat Protection Solutions
- **IDS:** Intrusion Detection System
- **SMEs:** Small and Medium Enterprises
- **APTs:** advanced persistent threats

Definition of Terms

- **Endpoint:** An apparatus that links to a network and retrieves data, like a desktop, laptop, or mobile phone.
- **Encryption:** The method of transforming information into a code to stop unwanted access.
- **Malware:** Software intended to interfere with, harm, or obtain unapproved access to a computer system.

CHAPTER 1: INTRODUCTION

1.1 Background

Businesses are starting to realize how important endpoints especially mobile devices are in data breaches as a result of the rising frequency of data leaks. These devices, which workers frequently utilize for work and personal use, might act as entry points for illegal access to private data. Because of this, enterprises need to give endpoint security top priority in order to safeguard their data assets from possible attacks. The increasing dependence of organizations on mobile technology has necessitated the implementation of robust security mechanisms to mitigate the risks inherent in these devices.

According to recent studies, internal reasons are also responsible for the surge in data breaches, in addition to external threats. Intentional or inadvertent employee carelessness can result in serious security vulnerabilities. According to a recent study, "This pressing issue has caused the emergence of a significant market for various software products that provide endpoint data protection for these organizations" (Chandel et al., 2019). This expanding industry is a reflection of how urgently companies must look for cutting-edge solutions to strengthen their cybersecurity posture and protect sensitive data. Effective endpoint security measures are becoming necessary due to the rising frequency of data breaches, as shown in Table 1.1, "Global and Local Endpoint Threat Statistics."

Furthermore, established strategies for protecting private workplace data, like staff training initiatives, have not worked well enough. According to research, "employee training, which aims to promote the awareness of protecting the sensitive data of the organization, is not very useful"(Chandel et al., 2019). This emphasizes the need for integrated endpoint protection solutions that can successfully minimize risks and improve overall data security, and it also highlights the need for enterprises to investigate more efficacious tactics that surpass basic training.

1.2 Introduction

The rapid growth of cyber threats has transformed the global trade landscape, necessitating a reassessment of security measures by institutions. According to the World Economic Forum, "During the next ten years, cyberattacks are expected to become the second most severe threat for global commerce because to their continued growth in sophistication and size" (Karantzas & Patsakis, 2021). This worrying trend highlights how critical it is for businesses to deploy more sophisticated security measures given the increasing complexity of threats like advanced persistent threats (APTs).

Endpoint detection and response (EDR) systems are becoming essential tools in any organization's cybersecurity toolkit due to the increasing threats they face. By linking data and events from several endpoints, EDRs provide a comprehensive approach to security and enable enterprises to see oddities that traditional antivirus programs would overlook. "EDRs offer a more holistic approach to the security of an organization" (Karantzas & Patsakis, 2021) by evaluating and connecting individual events, which improves threat detection capabilities. Because cyber threats are dynamic, even with advances in EDR technology, these systems need to be reviewed and modified on a regular basis.

Table 1.2, "Comparison of Endpoint Security Solutions," which gives an overview of the efficacy of various techniques against advanced persistent threats (APTs), demonstrates the significance of evaluating various security solutions. By modeling attacks that mirror real threats, this research aims to acquire a better understanding of how effective EDR systems are against APTs. Through an analysis of EDRs' reactions to these sophisticated attacks, we hope to find any gaps or openings in the security procedures that are now in place. In the end, this study aims to inform businesses on the importance of adopting a proactive cybersecurity strategy, making sure they are ready to repel ever-more-complex threats in a more interconnected world.

1.3 Statement of the Problem

Attacks by advanced persistent threats, or APTs, are becoming a more serious danger to major corporations and governments. APTs, in contrast to standard hacker attacks, adhere to the "low and slow" approach, whereby attackers use a variety of attack channels to infiltrate target hosts and carry out a variety of attack phases, such as reconnaissance, lateral movement, post-exfiltration, and foothold establishment. "The ultimate aims of APT attacks are to steal sensitive data from users' office computers and storage devices, hinder the execution of regular server activity, and compromise the integrity of the core infrastructure" (Chen et al., 2023). Many businesses continue to depend on traditional security measures, which are ill-equipped to handle extended and covert incursions, in spite of these grave risks.

APT defense has made endpoint detection and response (EDR) systems indispensable; nonetheless, there are still a number of important issues that restrict their efficacy. One significant problem is that, according to Chen et al. (2023), "Existing data storage strategies are often not optimized based on the characteristics of provenance graphs, making it challenging both to rapidly respond to attacks in real-time query scenarios and to efficiently store text during post-event analysis." Because of their inability to react quickly enough to threats that arise in real time, companies become more vulnerable and experience delayed threat detection, which undermines their overall cybersecurity defenses.

Thus, the purpose of this study is to assess how well EDR systems defend against APT attacks and suggest fixes for these data management flaws. This study aims to create an optimized framework that improves an organization's ability to respond to sophisticated cyber-attacks by identifying the major gaps in current storage strategies and response times. With the help of this strategy, businesses will be able to reduce the long-term threats presented by APTs and strengthen their overall cybersecurity posture.

1.4 Proposed Solution

The purpose of this study is to investigate how well advanced data management frameworks function to improve endpoint detection and response (EDR) systems' capacity to identify and neutralize advanced persistent threats (APTs). "Provenance graphs are a valuable tool for capturing the causal linkages between system activities, as recent research has shown." (Chen et al., 2023). This makes security analysis more accurate and visible. Security analysts can detect malicious activity more quickly by using provenance graphs, which shortens the time it takes to respond to possible APT assaults.

To improve EDR systems, researchers worldwide have concentrated on refining data collecting, compression, and storage techniques. Chen et al. (2023) draw attention to the difficulty that many businesses still face in striking a balance between high data fidelity and effective data storage. “Regional improvements in data management that are adapted to particular threat and infrastructure environments hold potential for enhancing the efficiency of EDR systems in reducing APTs” (Alshamrani et al., 2019).

An optimal data management approach that incorporates these regional and worldwide developments will be suggested by this study. This concept seeks to offer more effective threat detection and response capabilities by streamlining data collecting and storage procedures within EDR systems, ensuring that organizations and governments may successfully lessen the impact of APTs. The suggested approach will take into account the most recent data management techniques rather than depending on antiquated technology, thereby addressing the dynamic nature of cybersecurity risks. Please consult Table 1.3, "Budget Allocation for Endpoint Security Project," for a breakdown of the funds needed to support the suggested framework for improved endpoint detection and response systems.

1.5 Objectives

This research has two main goals: a single overarching goal and a number of more focused goals. The aforementioned objectives are intended to direct research efforts towards comprehending and enhancing the efficacy of Endpoint Detection and Response (EDR) systems in countering Advanced Persistent Threats (APTs) within corporate environments.

To assess how well Endpoint Detection and Response (EDR) systems operate at preventing Advanced Persistent Threats (APTs) and to suggest a plan for enhancing enterprise cybersecurity. The specific objectives are:

- Understand Weaknesses of EDR System in detecting and Responding to APT Attacks. (Mellen, 2022)
- The ability of handling advanced cyber threats using EDR and data management systems on a global scale.
- Create a new data management framework to close the gap between current EDRs are more secure.
- To check the performance of different susceptibility prevention and APT attack spread analysis approaches using our data management framework.
- Evaluation of enhanced EDR systems deploying have on the overall security posture within enterprises over a period.

1.6 Research Questions

What particular shortcomings do Endpoint Detection and Response (EDR) systems have when it comes to identifying and countering Advanced Persistent Threat (APT) attacks?

How well do the data management and emergency response systems in place today handle sophisticated cyber threats globally?

What fresh approaches can be created to strengthen the defenses of current EDR systems against changing APT techniques?

What effect do different data management frameworks have on how well EDR systems stop APT attacks?

How do improved EDR systems affect an organization's overall security posture over time? (Alam and Wang, 2021).

1.7 Hypothesis

Organizations that use adversary emulation in proactive threat hunting will see a significant decrease in the effectiveness of Advanced Persistent Threat (APT) attacks "the proposed approach defines offensive security as a process of understanding the adversary and then building plans for launching attacks (Ajmal, Shah, Maple, Asghar, & Islam, 2021).

1.8 Justification

The objective of this study is to tackle the increasing threat presented by Advanced Persistent Threats (APTs), which have increased in sophistication and frequency. “These types of attacks are distinct from the common cyberattacks due to their long-term, stealthy nature, allowing attackers to persist within compromised systems for extended periods” (Karantzas & Patsakis, 2021). There are still a lot of vulnerabilities even though modern security measures, such Endpoint Detection and Response (EDR) systems, are made to recognize and stop these attacks. This research's contribution is to assess how well EDR systems defend against APT attacks by modeling actual attack scenarios. In doing so, the study will highlight potential security flaws that companies may encounter and assist companies in strengthening their cybersecurity defenses.

Small and medium-sized businesses (SMEs) will greatly benefit from the research's findings since they will be better equipped to identify APTs early in the process, averting huge financial and data losses. Additionally, it will offer a thorough examination of the shortcomings of the current EDR systems, adding to the larger body of knowledge on cybersecurity and useful applications for enterprise-level security. It is anticipated that this study will give cybersecurity teams practical insights to strengthen their defenses against increasingly cunning hostile strategies. As highlighted by Karantzas and Patsakis (2021), the effectiveness of EDR systems in detecting APT attack vectors is crucial for maintaining robust organizational security.

1.9 Proposed Research and System Methodologies

Data provenance analysis is incorporated into the proposed technique to solve the inadequacies of traditional Endpoint Detection and Response (EDR) systems. Enhancing the validation and investigation of security alerts produced by EDR technology is the main objective of this project. Data provenance analysis can help in understanding the causal linkages between system events, which is necessary for accurately recognizing threats. Our method improves on current EDR frameworks by incorporating data provenance, guaranteeing a more successful and fast threat detection procedure.

This method is justified by its focus on leveraging data lineage to get around the shortcomings of traditional EDR systems. Data lineage gives security teams the ability to track the sources and movements of data across the system, which improves the context of security warnings. As recent study has shown, “EDR tools constantly monitor activities on end hosts and raise threat alerts if potentially-malicious behaviors are observed” (Hassan et al., 2020). Our approach enhances existing EDR frameworks and ensures a more effective and successful threat detection process by adding data provenance. The tactics for optimizing EDR systems against APTs are informed by the data shown in Tables 1.1 and 1.2, which also have an impact on the methodologies used in this study.

The stages of the research life cycle are as follows:

Planning and Exploration: Determine the difficulties that EDR systems are currently facing and develop research topics.

Development: Create and put into action the EDR system's suggested data lineage structure.

Assessment: Evaluate the efficacy of the new system through testing and validation.

Iterate: Based on input, make the required changes to improve system performance.

Reporting and Documentation: Gather information and present results in an extensive report.

1.10 Scope

The endpoint security issues that remote workers in many organizational settings encounter are the main topic of this study. The focus area is mostly urban and suburban areas where remote work is common. This affects a wide range of target consumers, including workers from large organizations and small- to medium-sized businesses (SMEs). The study will primarily focus on assessing how well endpoint security tools such as antivirus software, endpoint detection and response (EDR) systems, and the zero-trust security model protect remote users against common cybersecurity threats. As stated in the study, “with the shift towards remote work, organizations have become more vulnerable to cyber threats, necessitating a reevaluation of existing security frameworks” (Mandru, 2023).

1.11Budget

The project budget describes the expected costs for creating and putting into place the suggested Endpoint Detection and Response (EDR) systems framework. The estimated costs are broken down into the following sections:

1. Personnel Costs:

Research Team Salaries

Support Staff Wages

2. Materials and Supplies:

Software Licenses:

Security Tools:

3. Equipment:

Computers and Servers:

Networking Equipment:

4. Operational Costs:

Utilities (Internet, electricity):

Office Supplies:

5. Contingency Fund:

Reserve for Unexpected Expenses:

Total Estimated Budget:

As the project develops, this budget could change in response to actual requirements and costs. It seeks to guarantee sufficient funding for all project components that are essential to its successful execution and results.

1.12Schedule

The following crucial phases have been identified, and the project is scheduled to be finished in six months:

Planning and Research (Month 1): This month will be devoted to planning and identifying the current limitations of the Endpoint Detection and Response (EDR) systems. This means learning about Advanced Persistent Threats (APTs), reading reviews of relevant literature, and staying up to date on data management systems. Consultations with significant others will take place to gather requirements.

Months 2-3: Design of the Enhanced Data Management Framework Designing the suggested data management structure will be the focus of this step. This means creating models and methods to enhance the functionality of EDR systems. Collaborating with technology experts and security analysts will ensure that the framework conforms to the most recent industry standards.

Development and Implementation (Months 4-5): In this phase, the framework will be designed and integrated into an EDR system that is currently in place. The development of testing environments that imitate APT assaults will enable iterative testing and system enhancement.

Evaluation and Testing (Month 6): The goal of this final month is to determine how effectively the system performs when subjected to APT attacks that are simulated. There will be a comprehensive assessment that identifies the system's benefits and flags areas that require further work. Important parties will be provided with a well-written report.

Documentation and Reporting (End of Month 6): After the project is over, all findings, conclusions, and recommendations will be put together into a final report that will include instructions for implementing the framework that was developed, future recommendations, and documentation.

1.13Hardware and Software Requirements

In order to effectively execute the suggested EDR systems framework, the subsequent hardware and software prerequisites are required:

Hardware- Servers; Minimum specifications (e.g., CPU, RAM, Storage) Networking Equipment; Firewalls, routers, switches Workstations: For the research and development team (e.g., PCs with minimum specifications).

Software prerequisites- Operating System; (Name the version, such as Linux or Windows Server), EDR Software; (Include version and vendor), Tools for Data Management; (Name the program required to analyze the provenance of the data), Security Tools; (Any extra instruments for observation or testing).

These specifications will guarantee that the project gets the software and hardware support it needs to successfully accomplish its goals.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

The research on Endpoint Detection and Response (EDR) systems, both empirical and theoretical, will be reviewed in this chapter with an emphasis on how these systems defend against Advanced Persistent Threats (APTs). The review will point out the different approaches used by earlier researchers, underline the shortcomings of those approaches, and highlight the significant gaps in the literature that call for more research. The creation of a conceptual framework that demonstrates how many factors interact to affect the efficacy of EDR systems in cybersecurity will also be covered in this chapter.

2.2 Theoretical review/Conceptual Framework

A strong foundation for comprehending the difficulties and restrictions faced by EDR systems in thwarting APT assaults is provided by theoretical and empirical literature. This part makes connections between these studies and the research issues mentioned in Chapter 1, highlighting important discoveries on the efficacy of data management frameworks, the shortcomings of the EDR systems in place, and the approaches employed to identify cyberthreats.

2.2.1 Weaknesses of EDR Systems in Detecting APTs

Scholarly literature has extensively highlighted the inadequacy of conventional EDR systems in real-time detection and mitigation of APT attacks. Chen et al. (2023) draw attention to the shortcomings in data analysis and storage that prevent these systems from responding in a timely manner. These systems frequently produce enormous amounts of data, which overwhelms their capacity to quickly identify and neutralize sophisticated threats. In a similar vein, Alam and Wang (2021) draw attention to the fact that present EDR systems prioritize reactive security over preventive measures, allowing APTs to go undiscovered for extended periods of time.

2.2.2 Data Management and EDR Systems

The performance of EDR systems can be improved by improving data collection and storage, particularly in distributed infrastructures, as discussed by Alshamrani et al. (2019). The capacity of the EDR system to effectively respond to localized threats is limited by existing frameworks, which frequently presume uniform data storage strategies that do not take area variances into account (Karantzas & Patsakis, 2021). Enhancing EDR frameworks with localized techniques and data provenance can greatly boost their detection performance.

2.2.3 Theoretical Frameworks

According to Ajmal et al. (2021) the Defense-in-Depth Theory, a well-known framework for comprehending layered cybersecurity solutions, having many security layers—including EDR systems is necessary for a strong defense against APTs. The Cyber Kill Chain Framework, which describes the phases of a cyberattack, is another important hypothesis. Although they frequently miss early attack detection, EDR systems are crucial for spotting and eliminating threats in their later phases (Chen et al., 2023). Additionally, the Provenance Graph Theory is significant because it highlights the connections between system events through data provenance graphs, which gives security warnings meaning and increases the accuracy of threat detection (Hassan et al., 2020).

2.2.4 Conceptual Framework

The conceptual framework focuses on enhancing real-time threat detection and response capabilities by integrating sophisticated data management approaches into EDR systems. The EDR system performance is the dependent variable in this framework, and data management frameworks, regional modifications, and endpoint detection techniques are the main independent variables that affect it. The suggested model seeks to improve APT detection by strengthening these parameters, particularly in the early phases of the Cyber Kill Chain.

2.3 Critique of the Existing Literature

Even though the use of EDR systems has been well studied, there are still a lot of unanswered questions regarding the real-time reaction to APTs. While studies such as Mellen (2022) give a general overview of the limits of the EDR system, they do not offer workable, scalable remedies. Although Chen et al. (2023) highlight the significance of data provenance, few studies have addressed the difficulties in striking a balance between data accuracy and storage efficiency when it comes to real-time threat detection. Additionally, a number of studies' emphasis on reactive measures (Alam and Wang, 2021) implies that proactive cybersecurity methods are underemphasized, leaving firms open to long-term, undetected threats.

Furthermore, geographical variations in threat landscapes and cybersecurity infrastructure are frequently disregarded. Although Karantzas and Patsakis (2021) stress the importance of localized data management techniques,

2.4 Summary

Important empirical and theoretical research that highlight the shortcomings of EDR systems in identifying APTs have been examined in the literature study. To comprehend the importance of EDR systems in cybersecurity, a number of theoretical frameworks were studied, including Defense-in-Depth, the Cyber Kill Chain, and Provenance Graphs. It is evident that even while EDR systems are a valuable tool for thwarting advanced persistent threats (APTs), they still have a lot of difficulties with proactive threat prevention, data management, and real-time threat detection.

2.5 Research gaps

The literature review notes that although EDR technology has advanced significantly, there are still a number of holes that this study seeks to fill:

Real-time Response to APTs: The difficulties associated with real-time data storage and retrieval in the context of EDR systems are not adequately covered by current research (Chen et al., 2023). The goal of this project is to better understand how to organize data in order to improve threat detection in real time.

Regional Adaptations: The majority of research on EDR systems that is now available concentrates on broad frameworks, ignoring the significance of tailoring data management tactics to local infrastructure and threat environments (Karantzas and Patsakis, 2021).

Proactive vs. Reactive Security: APTs can remain undetected for extended periods of time since many EDR systems are built using a reactive approach to cybersecurity (Alam and Wang, 2021). In order to predict and neutralize threats before they cause major damage, this research will examine proactive solutions that can be incorporated into EDR systems.

References

Chandel, S., Dehghantanha, A., & Kharbat, F. (2019). Endpoint protection: Measuring the effectiveness of remediation technologies and methodologies for insider threat. In 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC) (pp. 239-244). IEEE.

Karantzas, G., & Patsakis, C. (2021). An empirical assessment of endpoint detection and response systems against advanced persistent threats attack vectors. Journal of Cybersecurity and Privacy, 1(3), * 387-421.

Chen, T., Li, Y., & Liu, X. (2023). System-Level Data Management for Endpoint Advanced Persistent Threat Detection: Issues, Challenges and Trends. Computers & Security, 112, 103485.

Alshamrani, A., Aljohani, N., & Alshehri, A. (2019). A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities. IEEE Communications Surveys & Tutorials, 21(2),* 1851-1877.

Mellen, B. (2022). Evolving Endpoint Detection and Response to Keep Up with Modern Threats. Forrester Research.

Alam, M., & Wang, L. (2021). The Effectiveness of Enhanced EDR Systems for Improving Overall Cybersecurity and Mitigating Risks Associated with Advanced Persistent Threats. Computers & Security, 112, 102499.

Ajmal, A. B., Shah, M. A., Maple, C., Asghar, M. N., & Islam, S. U. (2021). Offensive security: Towards proactive threat hunting via adversary emulation. IEEE Access, 9, 126023-126033.

Hassan, W. U., Bates, A., & Marino, D. (2020, May). Tactical provenance analysis for endpoint detection and response systems. In 2020 IEEE Symposium on Security and Privacy (SP) (pp. 1172-1189). IEEE.

Mandru, S. K. (2023). Endpoint security in remote work environments. North American Journal of Engineering Research, 5(1),* 1-12.

Karatanzas, G., & Patsakis, C. (2021). An empirical assessment of endpoint detection and response systems against advanced persistent threats attack vectors. Journal of Cybersecurity and Privacy, 1(3),* 387-421.

List of Tables

Figure 1.1: Global and Local Endpoint Threat Statistics

Threat type	**Global Incidents (2023)**	**Local Incidents (Kenya 2023)**	**%Increase from 2022**
Ransomware Attacks	500,000	12,000	30%
Phishing Attacks	1,200,000	25,000	45%
Malware Infections	1,000,000	15,000	25%
Data Breaches	100,000	3,000	20%

Figure 1.2: Comparison of Endpoint Protection Solutions

Solution Name	**Features**	**Cost (USD)**	**Compatibility**	**Effectiveness Rating**
Solution A	Malware detection, firewall, encryption	Ksh 20,000	Windows, Mac, Linux	4.5/5
Solution B	Antivirus, data loss prevention	Ksh 15,000	Windows only	4.0/5
Solution C	Threat intelligence, mobile protection	Ksh 30,000	Windows, Mac	4.7/5
Solution D	Endpoint detection and response	Ksh 25,000	Windows, Mac, Linux, iOS	4.8/5
Solution E	Network security, user behavior analytics	Ksh 40,000	All platforms	4.6/5

Figure 1.3 Comparison of Endpoint Security Solutions

Solution Name	Features	Pricing	Ease of Use	Support	Security Rating
Solution A	Antivirus, Firewall, VPN	Ksh 5,000/user/year	Easy	24/7 support	9/10
Solution B	Antivirus, EDR, Firewall	Ksh 7,500/user/year	Moderate	12/5 support	8/10
Solution C	Antivirus, VPN, Web, Filtering	Ksh 6,000/user/year	Easy	12/5 support	7/10
Solution D	EDR, SIEM, Threat Intelligence	Ksh 10,000/user/year	Difficult	24/7 support	9.5/10
Solution E	Antivirus, IDS, Firewall	Ksh 5,500/user/year	Moderate	12/5 support	8.5/10

Appendices

- Instruments

  The tools used for data gathering and analysis will have a big impact on how well your study on Endpoint Detection and Response (EDR) systems against Advanced Persistent Threats (APTs) goes. The tools necessary are: Questionnaires and surveys will be used to collect qualitative information from cybersecurity experts about the difficulties they encounter and the efficacy of the current EDR systems. Data collecting may be streamlined with tools like SurveyMonkey and Google Forms. Interviews: Speaking with cybersecurity specialists in semi-structured or structured interviews can give you a better understanding of the subtleties of data management frameworks and EDR efficacy. Case Studies: This method will enable a thorough examination of certain APT occurrences and the reactions of EDR systems, providing useful insights into their performance. Data Analysis Tools: To examine security event data produced by EDR systems, software tools like Splunk or ElasticSearch will be used. Patterns and correlations in threat detection and response effectiveness can be found with the aid of these technologies.

- Budget

  A successful budget is basic for guaranteeing that all viewpoints of the investigate venture are enough financed. The proposed budget incorporates: Staff Costs: This will cover pay rates for the inquire about group and back staff, guaranteeing that all group individuals are compensated for their commitments. Materials and Supplies: Costs related with computer program licenses for EDR frameworks, security apparatuses, and information administration applications will be included here. Permitting expenses can shift essentially, with a few commercial computer program costing thousands of dollars yearly. Hardware: Costs for computers, servers, and organizing hardware will be designated. Up-to-date equipment is fundamental for conducting dependable reenactments and information examination. Operational Costs: This envelops utilities, such as web and power, as well as office supplies, which are vital for day-to-day operations. Possibility Support: A save for unforeseen costs, ordinarily around 10-15% of the entire budget, ought to be included to account for any unanticipated challenges.

- Work Arrangement

  A well-defined work arrange is vital for the convenient completion of the investigate venture. The work arrange incorporates the taking after stages: Arranging and Inquire about (Month 1): Center on recognizing current impediments in EDR frameworks, understanding APTs, and looking into important writing. This stage will moreover include partner interviews to accumulate necessities. Plan (Months 2-3): Create the improved information administration system. Collaboration with innovation specialists will guarantee that the system adjusts with the most recent industry measures.

Improvement and Execution (Months 4-5): Plan and coordinated the unused system into existing EDR frameworks. Make testing situations to mimic Well-suited assaults, encouraging iterative testing and refinements. Assessment and Testing (Month 6): Survey the execution of the framework against reenacted Able assaults. Conduct a comprehensive assessment to distinguish qualities and shortcomings, eventually driving to proposals for change. Documentation and Detailing (Conclusion of Month 6): Compile discoveries, conclusions, and suggestions into a last report. This will serve as a direct for actualizing the unused system and recommend future inquire about headings.