Ahmad Maghaireh 23110205

Fadia Alaeddin

Technical Report

Green Circle

This report examines the integration of an AI-driven threat detection and response system at Green Circle, a cybersecurity firm based in Amman, Jordan. It explores how AI technologies, such as machine learning and deep learning, can enhance real-time threat detection and incident response. Through survey data from Green Circle employees and a review of current AI cybersecurity trends, the report identifies key challenges and opportunities in implementing AI solutions. It provides actionable recommendations to optimize the system’s effectiveness, address security risks, and improve overall efficiency, ensuring a seamless transition to an AI-powered cybersecurity infrastructure.

# **Introduction**

In computer science, Artificial Intelligence refers to a machine's ability in matching human intelligence in carrying out tasks. It involves technologies laid down that enable machines to simulate aspects of thought processes of a human being, which range from learning, reasoning, problem-solving, perception, and language understanding. AI systems rely on huge datasets, complex algorithms, and high computational power to process data and make independent decisions. The subset of AI, called machine learning, comprises systems that automatically improve their performances with experience-that is, from the data-without explicit programming. Deep learning is another important domain in which models of neural networks of the human brain are utilized to carry out difficult jobs, such as the recognition of images and speech. AI application is not limited to data; besides a great number of fancy models, the whole computation infrastructure should be able to process this data in real-time.

These technologies find increasing applications in various organizations these days for operation efficiency and to develop innovations. Big data analytics is the core tool associated with AI-driven solutions. This deals with handling big dataset size to extract useful insights. Machine learning platforms, ranging from TensorFlow and PyTorch [10] to others, are some of the important frameworks where one can build and then deploy AI models so that they learn from data. Besides that, AI-based applications-from customer service bots to predictive manufacturing maintenance tools-are routine for the automation and optimization of a lot of other business functions. For example, AI technologies are being integrated into SIEM systems in cybersecurity for tracing network traffic and detecting real-time potential cyber threats. Additionally, cloud-based AI platforms like Amazon Web Services and Microsoft Azure have catalyzed the deployment of organizational AI applications with the much-needed computing power and scalability.

This demands advanced storage and processing capabilities to bring AI technologies into realities and leverage cloud infrastructure with distributed computing in order to process large blocks of data that are demanded in training AI models. Equipped with such technologies, any organization is better able to unlock insights from data more effectively, make better decisions, and drive operational efficiency.

The integration of AI technologies will surely enhance operational efficiencies across all sectors significantly. For instance, AI systems would optimize supply chains in the manufacturing industry to a greater extent besides reducing downtime by predictive maintenance. Similarly, AI models will aid diagnosis and overall management of patients in healthcare, which would result in a decision-making process with much lesser utilization of time and resources. AI in cybersecurity helps organizations detect potential threats in real time, abnormal behavior, and automatic incident response, hence reducing identification and mitigation times drastically. Routine tasks can be automated in both internal and external networks with the help of AI. It can analyze large volumes of data, draws actionable insights from it, and makes a company truly agile, thereby saving human effort from various executions of such complicated tasks.

This could be targeting Green Circle's identification of threats through AI technologies to fast-track breaching in security and possible vulnerabilities for making operations of the company generally more efficient. Monitoring huge volumes of network traffic flow, discovering patterns that can depict a probable threat, and taking action against such an attack all by itself: this would reduce dependence on human monitoring and facilitate the pace of threat mitigation.

This report, therefore, investigates how AI technologies influence operational efficiency through a study of possible integrations of AI-driven threat detection and response systems within Green Circle. This will involve the contribution of AI in cybersecurity operations at Green Circle, real-time threat detection and response contribution, and finally the general security posture of the organization. The present report, therefore, tries to discuss the advantages and challenges as accrued from the implementation perspective, based on primary data gathered from Green Circle's management and employees.

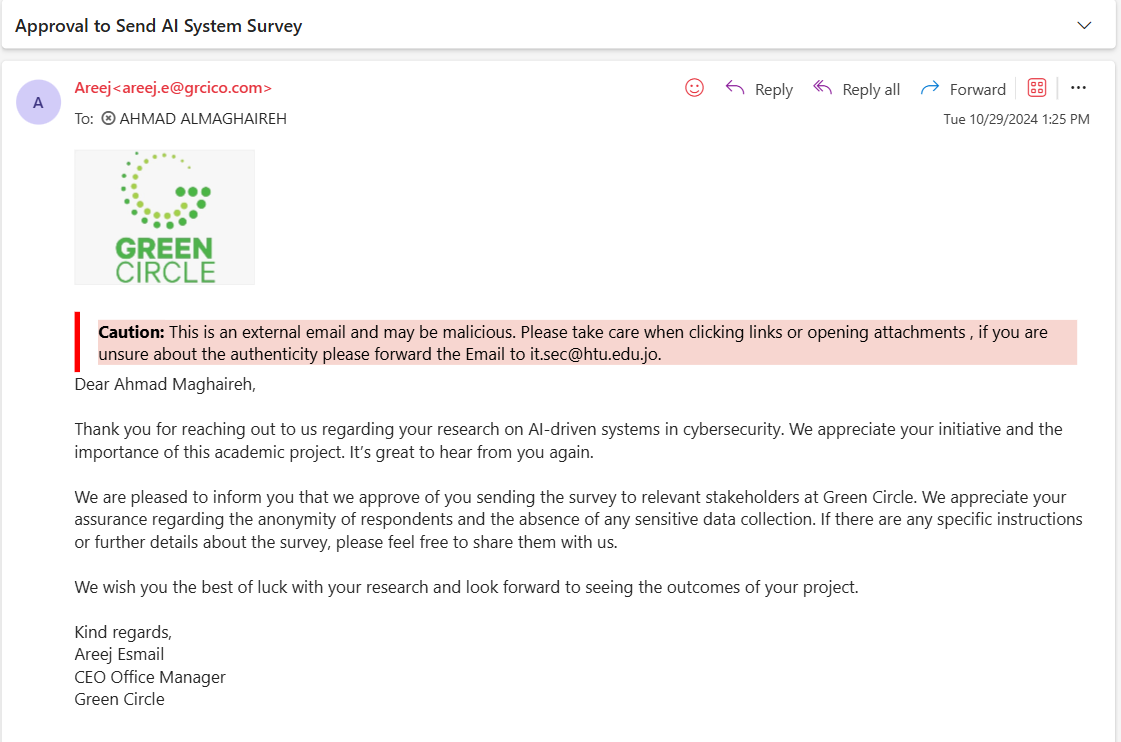
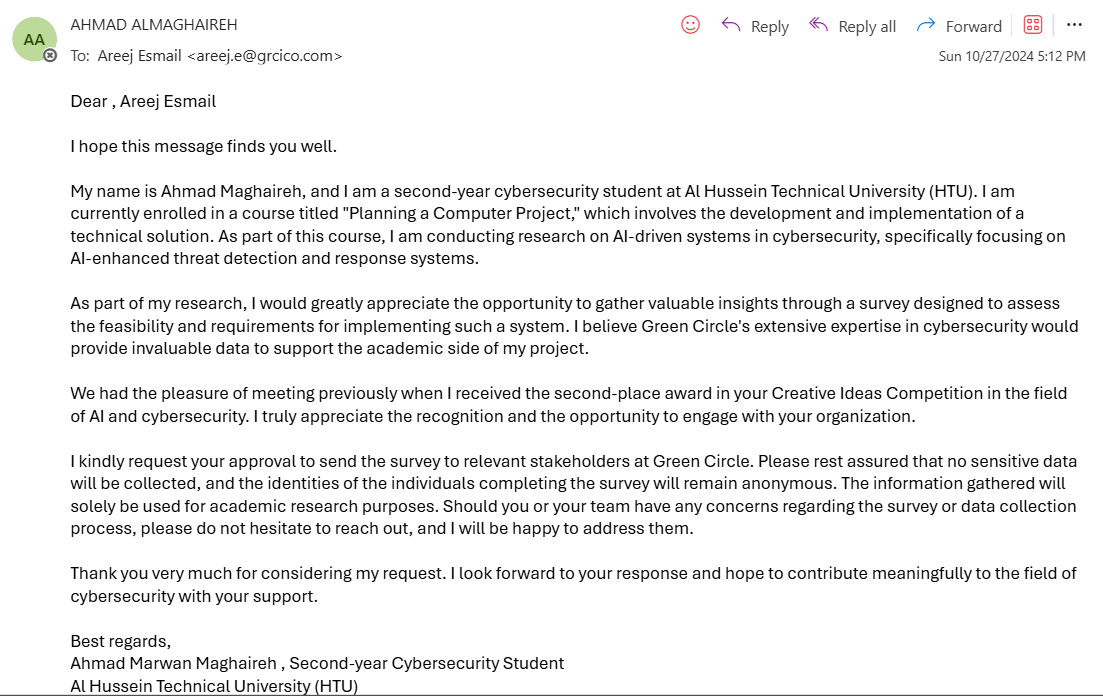
# **Organizational Study**

## **Identify the organization**

For this project, I selected **Green Circle**, a cybersecurity firm based in Amman, Jordan, as the organization for my study. Green Circle specializes in providing advanced cybersecurity solutions, including Security Analytics, Intrusion Detection, SIEM & Log Data Analysis, File Integrity Monitoring, Vulnerability & Penetration Testing, Configuration Assessment and Hardening, and Incident Response. The organization focuses on protecting businesses from cyber threats by offering customized security services tailored to each client's needs.

More about Green Circle : [1]

To begin, I reached out to Green Circle to obtain their consent for the study and to gather information about their current operations and challenges. The following is a sample of the email communication sent to them:



A screenshot of a computer

Description automatically generated

Green Circle responded positively, indicating their willingness to participate in the study. The organization also provided access to relevant stakeholders, including management and employees involved in cybersecurity operations, to gather insights for the research.

## **Features and the operational areas of the selected organization**

Business Features:

1. Business Ownership:

Green Circle will be a private limited company, LTD. It will enable the ownership structure of this business to retain control within the ring-fenced group of investors and shareholders. Besides, it protects personal assets from business risk because of limited liability, something hugely important for a cybersecurity company like itself dealing in sensitive data that is most probably liable on account of security breaches.

2. Industry Sector:

The green circle works in the technology industry, or rather, in the line of cybersecurity. When one is providing a service for protection against IT infrastructure, the firm is considered a tertiary industry. This industry has been constantly growing since there are more and more cyber threats, which naturally means that people need stronger security.

3. Product and Service Offering:

The Green Circle offers both products and services; its products are cybersecurity software, which includes Sinarra by Green Circle [2], [3], while services incorporate consulting, threat detection, and managed security services [4]. Here, it integrates both products and services to offer comprehensive solutions that answer challenging demands set by its customers in different fields.

4. Diversification:

Green Circle: We will help it adopt a related diversification strategy whereby its offerings shall be expanded with AI and machine learning on top of pure cybersecurity services. This would enable a step by Green Circle to enrich the product basket for serving clients with diversified needs and thereby establish itself as a leading player in this advanced cybersecurity solution space.

5. Compliance and Regulations:

The company makes sure that everything according to specific industry regulations, like GDPR or any data protection acts, is complied with. Compliance plays a major part in this industry since businesses operating here often have to manage very sensitive client information.

Operational Areas and Contribution to Green Circle's Purpose:

GC operates on the basis of a few main business functions: "Advanced Cybersecurity Solutions" is the purpose, supported, respectively, by direct functions of:

1. Human Resources:

Human resources will be able to identify, recruit, and train high-caliber cybersecurity personnel; similarly, high-caliber cybersecurity personnel further develop the firm's key talents to keep pace with rapid changes in the technologies and cybersecurity threats. In such a light, the role of HR becomes immensely important with respect to training, development, and retention of employees while delivering quality services at Green Circle.

2. Research and Development:

At Green Circle, innovation is deeply rooted in R&D. The organization invests in research for new cybersecurity technologies and AI-driven solutions to keep pace with emerging threats. That's how, through continuous product and service enhancement via R&D, Green Circle has made sure its offerings remain effective and relevant in the face of a rapidly changing cybersecurity environment.

3. Sales and Marketing:

This encompasses hard work from both the sales and marketing teams in placing Green Circle's products and services in the highly competitive cybersecurity market. These two sections work in close collaboration in acquiring new clients, maintaining client relationships, and communicating the value of Green Circle's solutions. The marketing function should ensure that the company's brand is recognized as a leading cybersecurity company to contribute toward business growth.

## **Stakeholders**

Internal Stakeholders

The internal stakeholders are involved with Green Circle in terms of its day-to-day operations and decision-making processes. These include management, employees, and shareholders.

1. Management

Role:

Management must identify the general trend, make major decisions in the processes of operation, and ensure the orientation of all functions of the business to organizational goals.

Impact on Success:

Decision Making: Managers would make key resource decisions, product development initiatives, and how to engage clients, affecting Green Circle's profitability and growth.

Operational Efficiency: They make the company function properly with good managerial skills. It will minimize your costs while increasing your productivity.

The solution is resilient to companies by finding and reducing cybersecurity risks, and that is the job of the managers.

2. Labor

Role:

The staff perform the tasks, make developments around cybersecurity, and care for the customers.

Impact on Success:

• Productivity and Innovation: The highly expert employees contribute to innovating more value-added cybersecurity solutioning for customer needs, hence strengthening the market position of Green Circle.

• Customer Satisfaction: The quality of customer service provided by employees directly impacts client retention and brand reputation.

• Operational Stability: Motivated and well-trained employees ensure smooth day-to-day operations, reducing errors and improving service quality.

3. Shareholders

Role:

The shareholders contribute the equity needed to operate Green Circle and all of its growth projects.

Impact on Success:

Funding and Investment: Shareholders’ investments enable Green Circle to expand its R&D capabilities, adopt new technologies, and enter new markets.

Influence of Strategy: Shareholders have their influence on strategic goals and objectives by voting on major decisions and ensuring overseeing.

Financial expectations: this again would incentivize the company to seek profitability and growth in a non-destructive way.

External Stakeholders

External stakeholders, though not directly involved in daily operations, significantly impact Green Circle's success through their interactions with the company. These include suppliers, customers, government agencies, and the local community.

1. Consumer

Role

The customers are those who purchase cybersecurity solutions and services from Green Circle.

Impact on Success:

Value Creation: Revenue comes from the customers; therefore, customer satisfaction and retention are very crucial sides of the company's financial perspective.

Feedback and Improvement: Customer response would help Green Circle enhance its product to update and make it more competitive in the market.

Brand Reputation: This defines how good Green Circle is and thus can gain more clients to increase business.

2. Sellers

Function:

These include providers of hardware, software, and other materials required by Green Circle.

Impact on Success:

Operational Continuity: Reliable vendors secure for Green Circle good-quality supplies and raw materials, ensuring thereby continuity of service provision.

Cost Control: Cost of supply and its quality will affect the overall cost of operations and profit margin.

Innovation support: suppliers at the state of the art edge actually support companies in developing cybersecurity solutions.

3. Government Agencies

Position:

Such agencies regulate the operation of Green Circle and ensure observance of cybersecurity laws and regulations.

Impact on Success:

Regulatory Compliance: Fulfilling government regulations assists Green Circle in avoiding legal penalties and keeps it qualified for its operating license.

Grants and Funding: To add to that, governmental grants and incentives are also provided for research and development.

Market Impact: Changes in government policies on data protection might open up new opportunities or challenges for Green Circle.

4. Local Community Role: This would include all those people and organizations in the vicinity where Green Circle exists. Impact on Success: Social Responsibility: These community projects further establish Green Circle as a socially responsible organization. Human Resources: This offers a supply of potential labor in the local population. It will affect attracting qualified talent to the organization. Public Support: Good relations mean positivity in the community, hence increased support towards the operations and growth of the company.

## **Challenges to the success of the organization's business**

1. Change Management Challenges

Change management is important if Green Circle is to stay competitive, expand, and adapt to new technologies and changing market conditions. However, change management poses a number of challenges:

Planned Changes

Expansion and Diversification:

As Green Circle looks to expand its operations and diversify its service offerings, it is faced with challenges of scaling up the infrastructure, managing increased workloads, and maintaining service quality.

System Upgrades:

Upgrading cybersecurity systems is necessary in order to keep up with the evolving threats. However, it is difficult to deploy new systems without disrupting normal operations.

Method of Execution

Green Circle can choose from several system changeover strategies when deploying new technologies:

Parallel Changeover: The running of old and new systems concurrently increases costs and resource requirements.

Direct Changeover: This is a high-risk approach if the new system has not been fully tested.

Pilot Changeover: Less risky as it means first testing the system in one place then delaying full implementation.

Phase Changeover: One module at a time reduces risk but may take longer to complete.

Challenges:

Resistance to Change: Workers may show resistance to changes for several reasons, including the loss of jobs, being unaccustomed to new systems, or lack of involvement in decision-making.

Training: A shortage of adequate staff training about the new systems inevitably leads to low production accompanied by high chances of faults.

Communication Breakdown: Inadequate communication of the change plans can lead to ambiguity and diminish employee morale.

2. Laws and Industry Standards

Green Circle operates in a highly regulated industry, and the laws on cybersecurity and data protection are incredibly stringent. Compliance is mandatory but very hard to achieve.

Statutory Law:

Data Protection Laws: The necessity to adhere to laws in the likes of the GDPR or local data privacy regulation in Jordan increases operational costs.

Compliance: Adherence to industry-recognized standards, such as ISO 27001, requires continued investment in both security infrastructure and staff training.

Challenges:

Higher costs: Legislative compliance usually requires high investments in training, upgrading systems, and audits.

Operational Constraints: The tight regulations squeeze operational flexibility and lead to even more administrative work.

Non-compliance penalties: There could be steep fines, lawsuits, and reputational damage for those who do not comply with the regulations.

3. Communication of Change to Stakeholders

Effective communication is important to ensure stakeholders understand the need for change and support its implementation. Here are some of the challenges in communications that Green Circle faces:

Tailoring Communication: The different stakeholders, whether employees, customers, or investors, have different informational needs and preferences for communication.

Timely Communication: Delays in communicating the plans for change can lead to confusion, rumors, and resistance.

Engaging Remote Teams: With a potentially global workforce, it is challenging to engage remote employees and maintain consistent communication across all locations.

4. Management of Stakeholders

Effective management of stakeholder expectations and involvement, before, during, and after the change, is central to the success of Green Circle's initiatives.

Before the Change

Stakeholder Analysis: Identification of stakeholders, their level of influence, and their concerns.

Setting Clear Objectives: Communicate what the goals of the change are and how it fits in with the company's mission.

Engaging Key Stakeholders: Engage key stakeholders upfront to ensure buy-in and address any of their concerns.

During the Change

Training and Support: To correctly train the employees so they can easily put the new systems or processes in practice.

Monitoring Progress: Regularly monitor the implementation process and address any issues that arise.

Keep all stakeholders informed about the progress, milestones, and any changes made to the original plan.

After the Change:

Providing Ongoing Support: Offer continued support to employees and customers to address any post-implementation issues.

Evaluation of Success: Determine if the change achieved the expected result and solicit feedback from stakeholders.

Recognition of Efforts: Acknowledge and celebrate stakeholders' contributions in order to create goodwill and motivation for future changes.

5. Information Security Challenges As a cybersecurity firm, Green Circle must prioritize information security to protect sensitive data and maintain client trust. However, security challenges can threaten its success: Challenges: Data Breaches: Incompetent security measures give rise to data breaches, which translate into loss of money and damage to reputation. Loss of Intellectual Property: A cyber attack can expose proprietary information and hand an advantage to competitors. Hidden Costs: The hidden costs of security incidents would include the fees of litigation, compensation to customers, and an increase in insurance premiums. Impact on Success: Revenue Loss: A massive security breach will translate to lost business and reduced income. Brand Reputation Damage: A poor track record may damage the Green Circle brand image and become very challenging to attract new customers. Customer Trust: A solid security profile is indispensable to holding customer trust, a must for any long-term success.

## **Business Requirements**

**Business Requirements for Green Circle's AI-Driven Threat Detection and Response System**

**1. Financial Requirements**

* **Budget Limitations:**  
  Green Circle has allocated a budget of **$35,000** for the project. This budget must cover:

Procurement of hardware and software.

Licensing fees for AI-based cybersecurity tools.

Staff training and development.

Maintenance and support costs for the first year.

* **Cost Management:**  
  The project must adhere to a detailed cost management plan to avoid budget overruns.

**After questioning the organization, there limit is 30,000 which is below our expectations , this should be discussed with the organization to find solutions either to raise there budget or lower our cost**

**2. Time Requirements**

* **Project Timeline:**  
  The project must be completed within **9 months** to align with Green Circle’s strategic goal of launching the new system by the **end of Q3 2025**.
* **Milestones:**  
  Key project milestones include:

**Month 1-2:** Finalize project requirements and select vendors.

**Month 3-4:** Procure and install new hardware and software.

**Month 5-6:** Configure and integrate the AI system with existing infrastructure.

**Month 7-8:** Conduct testing and quality assurance.

**Month 9:** Deploy the system and provide employee training.

**3. Resource Requirements**

* **Human Resources:**  
  To ensure project success, the following additional personnel are required:

**Two AI specialists** to develop and customize the threat detection algorithms.

**One cybersecurity analyst** to monitor system performance and identify potential vulnerabilities.

**One project manager** to oversee project implementation and ensure adherence to the timeline and budget.

* **Training Requirements:**  
  All relevant employees must undergo comprehensive training on the new system, including:

AI system operation and management.

Data interpretation and response protocols.

**4. Technical Requirements**

* **Hardware Requirements:**

**High-performance servers** to support AI computation and data processing.

**Backup and recovery systems** to ensure business continuity in case of system failure.

**Network upgrades** to handle increased data traffic and enhance security.

* **Software Requirements:**

AI-based threat detection software with machine learning capabilities.

Integration with existing Security Information and Event Management (SIEM) systems.

Data encryption and secure communication protocols.

**5. Scope Requirements**

* **Scope of the Project:**

Implement an AI-driven system capable of identifying, analyzing, and responding to cyber threats in real-time.

Integrate the system with Green Circle’s existing cybersecurity infrastructure.

Provide automated reporting and analytics to support decision-making.

* **Scope Limitations:**

The project will focus on **internal IT infrastructure and client networks** but will not extend to third-party vendor systems or external cloud environments during the initial phase.

**6. Quality Requirements**

* **System Reliability:**  
  The system must achieve **99.9% uptime** to ensure continuous threat monitoring and response.
* **Detection Accuracy:**  
  The AI system must maintain a **false positive rate below 5%** to minimize unnecessary alerts and focus on genuine threats.
* **Compliance:**  
  The system must comply with industry standards such as **ISO 27001** and local data protection laws in Jordan.

**7. Risk Management Requirements**

* **Risk Mitigation:**  
  A risk management plan must be developed to address potential risks such as:

Delays in hardware or software delivery.

Resistance from employees to adopt the new system.

Potential security vulnerabilities during system integration.

# **Research Study**

## **Research Overview**

To investigate the requirements, challenges, and perceptions surrounding the implementation of an AI-driven threat detection and response system for Green Circle, I conducted a small-scale research study using both **qualitative** and **quantitative** research methods. This research aimed to gather primary data from various stakeholders, including both management/C-level executives and technical staff, in order to understand their needs, concerns, and readiness for AI adoption in cybersecurity.

* **Research Methodology**

The research utilized a **mixed-methods approach**, incorporating both **surveys** and **open-ended interviews**. This methodology allowed for a comprehensive understanding of organizational perspectives by combining numerical data with in-depth qualitative insights.

1. **Quantitative Method: Survey** A survey was designed to gather structured data on various aspects of AI-driven threat detection systems. The survey included both closed-ended questions (for quantitative analysis) and open-ended questions (for qualitative analysis). It was divided into several sections:

**Background Information**: Questions regarding the role, experience, and familiarity of respondents with AI-driven security systems.

**Product Requirements**: Questions to gauge the importance of different features, such as real-time threat detection and predictive analytics.

**Product Features**: Focused on the specific features respondents would prioritize in an AI-driven system.

**Resistance to AI Implementation**: Addressed concerns or barriers such as cost, complexity, and resistance to AI adoption.

The survey was distributed via a Google Forms link to ensure ease of access and to streamline data collection across various roles within the organization.

**Survey questions close-ended :**

**Note: question 14 is closed-ended but I kept it to keep the sequence and the context of the questions**

**a. Collecting Information about the Survey Responders**

**1. What is your role within the organization?**

**- IT Staff**

**- Security Analyst**

**- Network Administrator**

**- Systems Administrator**

**- financial department**

**- Manager or C level**

**2. How many years of experience do you have in the cybersecurity field?**

**- 0-2 years**

**- 3-5 years**

**- 6-10 years**

**- 10+ years**

**3. What is your gender?**

**- Male**

**- Female**

**- Prefer not to say**

**4. Have you previously worked with AI-driven security systems?**

**- Yes**

**- No**

**5. How would you rate your knowledge of AI in cybersecurity?**

**- Beginner**

**- Intermediate**

**- Advanced**

**b. Determining Product Requirements of the Proposed AI System**

**6. How important is real-time threat detection to your organization's security operations?**

**- Not important**

**- Slightly important**

**- Moderately important**

**- Very important**

**- Critical**

**7. What level of automation would you expect from the AI-driven threat detection system?**

**- Manual with minimal automation**

**- Some automated functions**

**- Fully automated with human oversight**

**- Completely autonomous**

**8. How important is it for the AI system to provide predictive analytics for potential threats?**

**- Not important**

**- Slightly important**

**- Moderately important**

**- Very important**

**- Critical**

**9. What types of threats should the AI system be able to detect?**

**- Phishing attacks**

**- Malware**

**- Insider threats**

**- Denial of Service (DoS) attacks**

**- Data exfiltration**

**10. How critical is the integration of AI with your current cybersecurity tools and infrastructure?**

**- Not critical**

**- Somewhat critical**

**- Moderately critical**

**- Very critical**

**- Essential**

**c. Determining Product Features of the Proposed AI System**

**11. What features would you prioritize for the AI-driven threat detection system? (Select up to 3 features)**

**- Real-time threat detection**

**- Automated incident response**

**- Behavioral analysis of users and devices**

**- Predictive threat analysis**

**- Data encryption and protection**

**- Multi-platform integration**

**- User behavior analytics**

**12. What data sources would you like the AI system to analyze to detect potential threats? (Select up to 3)**

**- Network logs**

**- Endpoint data**

**- Cloud-based data**

**- Email logs**

**- Web traffic**

**- Application logs**

**13. How important is it for the system to offer detailed reporting and dashboards?**

**- Not important**

**- Slightly important**

**- Moderately important**

**- Very important**

**- Essential**

**d. Understanding Resistance Against the AI System**

**14. What concerns would you have about implementing an AI-driven threat detection system? (open-ended for staff )**

**15. How likely is it that your organization will be resistant to adopting AI for threat detection and response?**

**- Not at all likely**

**- Unlikely**

**- Neutral**

**- Likely**

**- Very likely**

**Survey Link**: <https://forms.gle/demztrnAe7LdG4Df6>

1. **Qualitative Method: Interviews with Management/C-level Executives** In addition to the survey, open-ended interview questions were designed for management and C-level executives to gather more detailed insights about strategic goals, challenges, and expectations regarding the integration of AI into the organization's cybersecurity infrastructure. These interviews focused on organizational concerns, ethical considerations, and forward-looking visions for AI's role in enhancing security posture.

**Open-ended Interview Question** for Staff:

14. What concerns would you have about implementing an AI-driven threat detection system? (open-ended for staff )

**Open-ended Interview Questions** for Management:

* + What is the budget range allocated for the development and implementation of the AI-driven threat detection and response system?
  + What is the expected timeline for implementing the proposed AI system, from development to full deployment?
  + Are there any specific cybersecurity challenges or threats that your organization is currently facing, which the new AI system should focus on?
  + What are the primary goals you hope to achieve with the integration of AI into your cybersecurity infrastructure?
  + What concerns do you have about integrating AI into your existing security systems and workflows?
  + What level of customization or flexibility would you expect from the AI-driven threat detection system to meet your organization's unique needs?
  + How do you plan to handle any potential ethical or privacy concerns arising from the use of AI in cybersecurity?
  + What risks or challenges do you foresee in training and maintaining the AI-driven system, especially concerning staff adaptation and performance monitoring?
  + How do you envision AI enhancing the organization’s overall security posture in the coming years?
* **Sampling Techniques**

To ensure that the survey results and interview data were representative of the organization’s diverse roles, a **purposive sampling** technique was employed. The survey targeted employees across different functions, including:

* IT staff
* Security analysts
* Network administrators
* Systems administrators
* Financial department personnel
* Managers or C-level executives

Respondents were selected based on their involvement in the cybersecurity decision-making process or their role in implementing and managing security measures within the organization. This targeted approach ensured that the survey captured insights from individuals with varying levels of expertise, perspectives, and responsibilities related to cybersecurity.

For the qualitative interviews, the sampling was further refined to include C-level executives and senior management who were involved in the strategic decision-making process. These individuals were crucial to understanding the broader organizational vision for AI integration and cybersecurity improvement.

* **Ethical Considerations**

Ethical considerations were central to the design and implementation of the research. The following measures were taken to ensure the research was conducted ethically:

1. **Informed Consent**:

All participants were provided with an explanation of the survey’s purpose, its voluntary nature, and how the data would be used.

Participants were informed that their responses would be confidential and anonymous, and they had the option to withdraw from the survey or interview at any time without consequences.

1. **Confidentiality**:

All responses collected through the survey were kept confidential. No personally identifiable information (PII) was gathered, and data was anonymized to protect participant identities.

Open-ended responses from the management interviews were anonymized, and sensitive information regarding internal policies, budgets, or strategies was not disclosed.

1. **Data Security**:

All survey data and interview responses were securely stored and protected. Only authorized researchers had access to the data to prevent unauthorized disclosure.

1. **Minimizing Harm**:

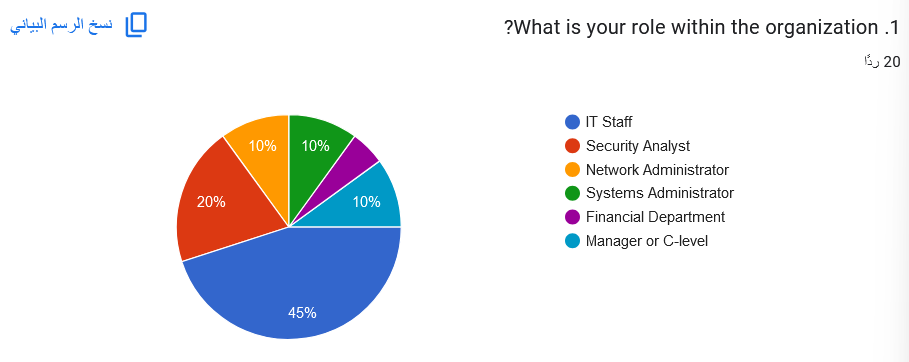
The survey and interviews were designed to be non-intrusive, and participants were not asked to share any personal or sensitive data unrelated to the research objectives.

1. **Transparency and Feedback**:

Participants were assured that the findings from the research would be used exclusively for the purpose of enhancing the AI-driven threat detection system’s design and implementation. Any potential feedback or results would be shared with participants in a summarized and anonymized form.

## **Analysis of Collected Data and Description of Generated Knowledge**

After cleaning the data from the unusable responses I ended up with 20 responses which are analyzed as follows :



Demographics of Respondents:

The majority of survey respondents belong to the IT Staff category (45%), indicating a strong representation of technical personnel who are directly involved in day-to-day IT operations. Security Analysts (20%) and Network/System Administrators (combined 20%) also have significant representation, suggesting that the survey primarily captures the views of those responsible for network security and infrastructure. The presence of Managerial or C-Level (10%) and Financial Department (5%) respondents highlights some strategic and financial perspectives in the responses.

A pie chart with different colored circles

Description automatically generated

The majority of respondents have 3-5 years of experience (38.9%), suggesting that the workforce is relatively experienced but still mid-career. A combined 44.4% have 0-2 years or 10+ years of experience, indicating a balanced distribution between early-career professionals and highly experienced individuals. This diversity in experience provides a well-rounded perspective on the organization’s cybersecurity needs.

A pie chart with numbers and a red circle

Description automatically generated

The gender distribution is almost perfectly balanced, with 55.6% male and 44.4% female respondents. This suggests that the survey captures perspectives from a diverse workforce and avoids gender bias in feedback.

A pie chart with red and blue circles

Description automatically generated

Half of the respondents have experience working with AI-driven security systems, while the other half do not. This indicates a split between those familiar with AI-based tools and those who might need training or exposure to such technologies, emphasizing the importance of user education and support during AI system implementation.A pie chart with text below

Description automatically generated

The majority of respondents classify themselves as Beginners (72.2%) in AI-related cybersecurity knowledge, while 27.8% rate themselves as Intermediate. No respondent considers themselves an advanced user. This highlights the need for training and capacity-building programs to improve AI knowledge within the organization

A pie chart with different colored circles

Description automatically generated

While 44.4% of respondents consider real-time threat detection only slightly important, a combined 50% find it at least moderately important or very important. This indicates a mixed view of real-time detection, suggesting some organizations may prioritize other aspects of security over immediate detection, while others see it as a key component.

A pie chart with text

Description automatically generated

Most respondents prefer some automated functions (61.1%) or full automation with human oversight (27.8%), indicating a desire for a balance between automation and human involvement. No respondents support a completely autonomous system, suggesting a lack of trust in fully independent AI systems.

A pie chart with different colored circles

Description automatically generated

50% of respondents consider predictive analytics only slightly important, while 50% view it as at least moderately or very important. This split indicates that while predictive analytics is valued by some, others might need further understanding of its potential benefits.

A graph with purple bars

Description automatically generated with medium confidence

The top three threats identified are phishing attacks, insider threats, and Denial of Service (DoS) attacks (all 66.7%). Malware and data exfiltration are also significant concerns but ranked slightly lower. This highlights a need for AI systems to focus on diverse threat detection capabilities, particularly for human-related and network-based threats.

A pie chart with different colored circles

Description automatically generated

Most respondents consider integration moderately critical (44.4%) or somewhat critical (38.9%), while a smaller portion views it as very critical or essential. This suggests that while integration is valued, it may not yet be seen as a top priority by all

A graph with purple bars

Description automatically generated

The most highly prioritized features for the AI-driven threat detection system are real-time threat detection, automated incident response, and behavioral analysis of users and devices, each receiving 61.1% of the votes. These features are critical to detecting and responding to threats promptly. The predictive threat analysis (38.9%) and multi-platform integration (38.9%) features also appear important, indicating that users value a flexible and forward-thinking system. Data encryption and user behavior analytics are less emphasized, though still noteworthy for a subset of respondents.

A graph with purple bars

Description automatically generated with medium confidence

The top three data sources for AI threat detection are network logs (77.8%), cloud-based data (72.2%), and endpoint data (61.1%). These are key areas for identifying threats and vulnerabilities in an organization’s infrastructure. Email logs (55.6%) are also considered important, reflecting a significant concern with phishing and other email-based threats. Web traffic and application logs are less prioritized, indicating that while useful, they are not seen as top priority for threat detection.

A pie chart with colorful circles

Description automatically generated

The majority of respondents view detailed reporting and dashboards as moderately important (55.6%) or slightly important (38.9%). Only a small percentage consider it very important or essential. This suggests that while reporting and visualization tools are valued, they may not be the highest priority compared to other features like real-time detection and incident response.

A pie chart with different colored circles

Description automatically generated

The majority of respondents are neutral (50%) or unlikely (38.9%) to resist adopting AI for threat detection and response, indicating a relatively open attitude toward AI implementation. Only a small percentage perceive resistance as a likely concern, with 5.6% seeing it as not at all likely and 5.6% as likely. This suggests that while resistance is not entirely absent, it is not a major barrier for the organization at this stage.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Job Security Concerns: A significant number of employees worry that AI might replace human roles, particularly in cybersecurity positions.

False Positives and System Reliability: There is notable concern about the potential for AI to generate false positives, which could lead to unnecessary alert fatigue and missed threats.

Training and Usability: Employees are uncertain about the ease of adopting AI and the training requirements associated with the new system.

Data Security and System Performance: Concerns about the handling of sensitive data and potential system slowdowns or resource strain were raised.

Trust and Control: There is a fear that AI could result in a loss of control over cybersecurity operations and lead to trust issues in AI-driven decisions.

While there are valid concerns, the overall sentiment about AI adoption within the organization seems to lean towards a low likelihood of resistance, with many respondents either neutral or optimistic about the process. However, the concerns raised should be carefully addressed during the implementation phase to ensure a smooth transition and buy-in from the staff.

A screenshot of a computer

Description automatically generated

The budget allocation for implementing the AI system is estimated to fall between $15,000 and $30,000, which reflects a mid-range investment in AI technology suitable for smaller or medium-sized organizations. This budget includes costs for hardware, software, and initial training. However, the final budget will heavily depend on the chosen vendor and the customization required, indicating that flexibility is key. The presence of a budget ceiling suggests that the organization is looking for a cost-effective solution, and that decisions around vendor selection will play a critical role in finalizing the investment. This figure does not seem to account for ongoing maintenance costs, future scaling, or additional personnel, which may require further investment later on.

A screenshot of a white box

Description automatically generated

The timeline to fully deploy the AI system is expected to span around one year, with 10 to 11 months allocated for initial rollout, testing, and staff training. The timeline emphasizes the need for a methodical and thorough implementation, ensuring that the AI system is properly integrated and that staff are adequately trained. However, the organization’s approach seems cautious, focusing on minimizing the risk of failure by allocating time for updates and optimizations post-deployment. The decision to extend beyond initial deployment reflects the recognition that AI systems require iterative refinement to ensure they perform optimally and stay relevant as the threat landscape evolves. Given the complexity of AI systems, the time allocated for testing and adjustments is a prudent approach.

A screenshot of a computer

Description automatically generated

The organization is currently most concerned with phishing and malware attacks, alongside insider threats and unauthorized data access. These areas highlight the organization’s need for an AI system that can detect not only external threats but also internal risks. The emphasis on phishing and malware indicates that the organization’s existing security measures may not be sophisticated enough to detect these threats in a timely manner, making AI's proactive capabilities a critical feature. The growing concern about insider threats and data access implies that a shift toward behavioral analysis and anomaly detection will be essential. These areas align with the capabilities of AI in cybersecurity, specifically in improving intrusion detection and identifying patterns indicative of unauthorized behavior.

A screenshot of a white box

Description automatically generated

The primary objectives for integrating AI are to reduce response times by 50% and improve detection of emerging and zero-day threats. These goals highlight the need for efficiency and effectiveness in the organization’s security operations. The specific focus on response time suggests that the organization experiences significant delays in reacting to incidents, which could be due to an over-reliance on manual processes or a lack of integration between existing tools. The inclusion of zero-day threats indicates a need for advanced threat intelligence, and the organization seems keen on reducing manual effort in detecting threats. The focus on response time and threat detection aligns with the core strengths of AI systems in automating tasks and identifying threats faster than traditional methods.

A screenshot of a chat

Description automatically generated

Concerns about integration and the potential for false positives highlight the challenges of introducing a new AI system into existing workflows. The complexity of some systems suggests that there may be resistance or difficulty in integrating new AI-driven solutions into the organization’s legacy infrastructure. The concern over false positives further suggests that there may be hesitation regarding the accuracy and reliability of the AI system. False positives could overwhelm staff, create inefficiencies, and potentially reduce trust in the system. It’s clear that the AI system needs to balance sensitivity and specificity to minimize disruptions to operations and ensure smooth integration.

A screenshot of a chat

Description automatically generated

The emphasis on customization reflects the organization’s need for a solution tailored to its industry-specific compliance and changing threat landscape. The flexibility to adapt to future changes in detection rules, regulations, or threat patterns is crucial for ensuring the long-term relevance of the system. This aligns with the broader need for AI systems to be agile and adaptable in the face of evolving cybersecurity risks. The AI system will need to offer modular and configurable features to ensure it can meet the dynamic demands of the organization. This also indicates that the organization expects the AI solution to evolve over time, integrating new capabilities and adjusting to emerging threats.

A screenshot of a computer

Description automatically generated

To address ethical and privacy concerns, the organization plans to implement strict data governance policies and conduct regular audits. This response suggests that privacy and compliance are top priorities, which is critical in cybersecurity, where trust and accountability are paramount. The approach to audits and stakeholder transparency reflects a focus on maintaining the trust of both internal and external stakeholders. This focus on privacy will be especially important as AI systems deal with large volumes of potentially sensitive data. The organization is prioritizing ethical AI use, ensuring that AI doesn't inadvertently compromise data privacy or security.

A white text with black text

Description automatically generated

Staff resistance to AI adoption is a common challenge, with concerns that it could create disruptions in workflows or cause discomfort among employees. Addressing this issue through ongoing training and clear communication will be essential for ensuring that the workforce adapts to the AI-driven changes. Additionally, maintaining the AI system and keeping it up-to-date with the latest threat intelligence may pose a logistical challenge, especially if the system is highly complex. These challenges point to the importance of staff engagement and support, not just during initial implementation, but as the system evolves.

A screenshot of a white and black text

Description automatically generated

The overarching vision for AI is to proactively mitigate risks and reduce manual effort in threat detection. AI is seen as a tool for enhancing threat intelligence and providing a more proactive approach to security. This suggests that the organization is seeking to move from a reactive security posture, where threats are dealt with after they occur, to a more predictive and preventive approach. AI is viewed as a strategic tool to strengthen the organization’s overall security posture, emphasizing the need for advanced tools to identify threats early and minimize human error in detecting and responding to them.

**Secondary data source (Papers/Articles )**

**Paper: Yaseen, A. (2023). "AI-Driven Threat Detection and Response: A Paradigm Shift in Cybersecurity" [5]**

**Question 1:**

How can qualitative research methods improve the integration of AI in cybersecurity?

**Answer:**  
Qualitative research methods, such as interviews, case studies, and focus groups with cybersecurity professionals, AI engineers, and stakeholders, provide critical insights into the operational challenges and human factors involved in implementing AI. These methods also help explore the interpretability of AI decisions and the collaboration between human operators and AI systems.

**Analysis:**  
Green Circle can benefit from incorporating qualitative research to better understand the contextual challenges of integrating AI in its cybersecurity framework. Engaging with professionals during system development will ensure smoother integration, greater transparency, and improved human-AI interaction.

**Question 2:**

What data sources are essential for developing effective AI-driven threat detection systems?

**Answer:**  
Key data sources include network traffic logs, system logs from servers and endpoints, malware repositories, and collaborative threat intelligence from cybersecurity communities. These sources provide valuable information for training, validating, and continuously improving AI models.

**Analysis:**  
Green Circle must establish comprehensive data collection pipelines to gather diverse datasets. Leveraging collaborative threat intelligence and industry partnerships will enhance the system's ability to detect and respond to evolving cyber threats.

**Paper: Salem, A.H., Azzam, S.M., Emam, O.E., et al. (2024). "Advancing Cybersecurity: A Comprehensive Review of AI-Driven Detection Techniques" [6]**

**Question 3:**

How do machine learning and deep learning models enhance threat detection?

**Answer:**  
Machine learning and deep learning models excel at detecting complex patterns in large datasets, enabling them to identify sophisticated threats such as zero-day attacks and APTs. These models can continuously learn from new data, improving detection accuracy over time.

**Analysis:**  
Green Circle should prioritize deploying deep learning models capable of handling large datasets and continuously learning. This approach will improve detection accuracy and adaptability, ensuring the organization stays ahead of advanced cyber threats.

**Question 4:**

What are the key limitations of AI-driven threat detection systems?

**Answer:**  
Challenges include model drift, data scarcity, high computational requirements, and the generation of false positives, which can lead to alert fatigue for security teams.

**Analysis:**  
Green Circle should adopt a hybrid threat detection approach that combines AI with human oversight to address false positives and model drift. Additionally, regular model updates and performance monitoring are essential for maintaining system effectiveness.

**Paper: Stanham, Lucia. (2024). "The Role of AI in Cybersecurity" [7]**

**Question 5:**

How do AI-driven systems manage large volumes of security data?

**Answer:**  
AI-driven systems can process vast amounts of security data in real-time, identifying anomalies and potential threats faster than manual methods. This reduces the workload on security teams and improves incident response times.

**Analysis:**  
Green Circle should integrate AI systems with its existing SIEM solutions to enable real-time data processing and threat detection. This will enhance the organization's ability to respond to threats promptly, reducing potential damage.

**Question 6:**

What ethical concerns arise from using AI in cybersecurity, and how can they be addressed?

**Answer:**  
Ethical concerns include data privacy, transparency of AI decisions, and potential biases in AI models. These can be mitigated by implementing data governance frameworks, ensuring model explainability, and conducting regular compliance audits.

**Analysis:**  
Green Circle must prioritize ethical considerations by adopting transparent and auditable AI systems. Establishing robust data governance policies will help build trust with clients and stakeholders while ensuring compliance with regulations.

**Paper: "AI in Cybersecurity: Revolutionizing Threat Detection." (2024). Data Science Dojo [8]**

**Question 7:**

How do AI systems improve real-time threat detection capabilities?

**Answer:**  
AI systems continuously analyze network traffic, system logs, and user behavior in real-time, identifying anomalies and potential threats more effectively than traditional methods.

**Analysis:**  
Green Circle should leverage AI to enable continuous monitoring and automated incident response. This will reduce the mean time to detect (MTTD) and mean time to respond (MTTR), enhancing overall security.

**Question 8:**

How do AI-driven systems overcome the limitations of traditional threat detection methods?

**Answer:**  
Traditional methods rely on predefined rules and signatures, which are ineffective against unknown threats. AI-driven systems, however, detect anomalies and patterns that indicate potential security breaches, even if they lack a known signature.

**Analysis:**  
Green Circle should transition from rule-based detection to anomaly-based AI models. This shift will enhance its ability to detect unknown and emerging threats, improving overall cybersecurity resilience.

**Paper: Sridhar Muppidi, I.F., and C.I.S. (2023). "AI in Cybersecurity: Yesterday’s Promise, Today’s Reality." [9]**

**Question 9:**

How do AI systems adapt to emerging and zero-day threats?

**Answer:**  
AI systems use unsupervised learning techniques and continuously update threat intelligence feeds to detect and respond to new threats without prior knowledge or signatures.

**Analysis:**  
Green Circle should integrate AI models that utilize unsupervised learning and continuously update them with real-time threat intelligence. This approach will ensure protection against emerging and zero-day threats.

**Question 10:**

What strategies are essential for the successful integration of AI-driven cybersecurity solutions?

**Answer:**  
A phased implementation approach, staff training, and collaboration with AI vendors are critical for successful integration. Continuous monitoring and feedback loops are also essential for ongoing system improvement.

**Analysis:**  
Green Circle should implement AI solutions in phases, starting with pilot projects. Providing training to staff and collaborating with vendors will ensure a smooth transition and maximize the effectiveness of the AI system.

## **Research Findings**

Based on the survey and secondary data analysis, the following findings interpret how AI-driven threat detection and response systems can align with Green Circle’s business requirements:

**1. Financial Requirements**

* **Budget Limitations**: The allocated budget of $30,000 is below expectations, and this budget must cover hardware, software, training, and support costs. The solution needs to be cost-effective without compromising essential features.
* **Finding**: The budget estimation of $15,000-$30,000 for AI systems is in line with mid-range investments. Green Circle needs to prioritize essential functionalities such as real-time threat detection and automated response while ensuring flexibility in vendor selection to stay within budget.

**2. Time Requirements**

* **Project Timeline**: A 9-month completion goal aligns with Green Circle’s strategic aims.
* **Finding**: Extending the implementation timeline to 10-11 months (from the estimated 9 months) seems prudent. Additional time will ensure proper integration and staff training, which is critical given that 50% of respondents have limited AI experience. Pilot testing and gradual deployment are vital for smooth integration.

**3. Resource Requirements**

* **Human Resources**: Two AI specialists and a project manager will be crucial for the system’s customization and oversight.
* **Finding**: Given the split in AI-related knowledge (72.2% are beginners), a substantial training program must be incorporated to upskill employees, particularly in AI system operation and data interpretation. The workforce is generally open to AI adoption, though the organization must address concerns regarding trust, training, and job security.

**4. Technical Requirements**

* **Hardware & Software**: AI-driven threat detection will require high-performance hardware and integration with existing SIEM systems.
* **Finding**: AI systems must be capable of processing real-time data from various sources like network logs, endpoints, and cloud-based data. Integration with existing infrastructure and ensuring system reliability (99.9% uptime) is essential to avoid disruptions. The need for real-time detection and automated incident response was emphasized by respondents (61.1%).

**5. Scope Requirements**

* **Scope Limitations**: The initial AI system will focus on internal IT infrastructure and exclude third-party vendor systems.
* **Finding**: The AI system must be adaptable and customizable to accommodate future integrations, ensuring that it can evolve with Green Circle’s security needs. Flexibility for handling emerging threats and evolving cybersecurity landscapes is necessary, as indicated by the priority on predictive analytics (50% view it as moderately or very important).

**6. Quality Requirements**

* **System Reliability & Detection Accuracy**: The AI system should minimize false positives and maintain high detection accuracy.
* **Finding**: Respondents highlighted the importance of avoiding alert fatigue due to false positives. A hybrid approach that combines AI capabilities with human oversight will be critical for maintaining detection accuracy and ensuring operational efficiency.

**7. Risk Management Requirements**

* **Risk Mitigation**: The implementation must address risks related to integration challenges, employee resistance, and potential system vulnerabilities.
* **Finding**: Addressing staff concerns about job security, trust, and system performance will be essential to minimize resistance. Clear communication, continuous training, and data security measures will help ensure successful adoption and mitigate risks.

**Alignment with Research Theme and Business Requirements:**

* **AI-Driven Detection**: AI systems excel in processing large volumes of data in real-time, offering Green Circle the ability to detect threats quickly and reduce response times, addressing core business needs around timely threat detection and incident response.
* **Real-Time Detection & Response**: According to the survey, the majority of respondents prioritize real-time threat detection and automated incident response. AI's ability to automate these functions aligns directly with Green Circle’s goal to enhance its cybersecurity capabilities.
* **AI Integration and Customization**: The integration of AI with existing infrastructure is crucial. While integration is moderately important to most respondents, a phased implementation approach (including pilots) will ensure smoother adoption and help minimize disruptions. Continuous learning and adaptation to new threats, as highlighted by papers on AI’s ability to handle zero-day threats, will improve the system’s resilience.

**New Requirements Based on Findings:**

**Staff Training & Support**: Extensive training is needed to overcome the gap in AI-related knowledge, ensuring that all relevant employees can operate the system effectively.

**Flexible Budget & Vendor Solutions**: Given the budget limitations, flexibility in vendor selection and cost management plans are necessary. Green Circle should prioritize cost-effective solutions that do not compromise key features like real-time detection and automated response.

# **References**

1. <https://grcico.com/about/>
2. <https://grcico.com/ar/cybertools/>
3. <https://sinnara-app.com/>
4. <https://grcico.com/solutions-green-circle/>
5. Yaseen, A. (2023) “AI-DRIVEN THREAT DETECTION AND RESPONSE: A PARADIGM SHIFT IN CYBERSECURITY”, *International Journal of Information and Cybersecurity*, 7(12), pp. 25–43. Available at: https://publications.dlpress.org/index.php/ijic/article/view/73 (Accessed: 1 November 2024)
6. Salem, A.H., Azzam, S.M., Emam, O.E. *et al.* Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. *J Big Data* **11**, 105 (2024). <https://doi.org/10.1186/s40537-024-00957-y>
7. stanham, lucia (2024) *The role of AI in Cybersecurity*, *CrowdStrike*. Available at: https://www.crowdstrike.com/en-us/cybersecurity-101/artificial-intelligence/ (Accessed: 01 November 2024).
8. *Ai in cybersecurity: Revolutionizing threat detection* (2024a) *Data Science Dojo*. Available at: https://datasciencedojo.com/blog/ai-in-cybersecurity/ (Accessed: 01 November 2024).
9. Sridhar Muppidi, I.F. and C.I.S. (2023) *AI in Cybersecurity: Yesterday’s promise, today’s reality*, *MIT Technology Review*. Available at: https://www.technologyreview.com/2023/05/24/1073395/ai-in-cybersecurity-yesterdays-promise-todays-reality/ (Accessed: 01 November 2024).