Scientific and Practical Cyber Security Journal (SPCSJ) 8(3): 8 – 20 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

A PROCESS FLOW MODEL FOR DYNAMIC ENTERPRISE NETWORK CYBER SECURITY ANALYSIS IN EASTERN AND CENTRAL UGANDA

Shariff MUGOYA[1], Twaibu SSEMWOGERERE[1], Godfrey ODONGTOO[1], Mwase ALI[2], and Gilbert Gilibrays OCEN[1]

[1]Department of Computer Engineering and Informatics, Faculty of Engineering, Busitema University, P.O. Box 236, Tororo, Uganda

[2]Department of Marketing and Management, Makerere University Business School, P.O. Box 1337, Kampala, Uganda

ABSTRACT: Several Enterprises are adopting Enterprise Networks due to their benefits like remote file storage, resource sharing, and improved communication. Due to a large number of target groups, cyber-attackers have exploited vulnerabilities in the Enterprise Networks to launch cyber-attacks on these networks thus resulting into data theft and financial losses to the enterprises. In this study a Dynamic Enterprise Network Cyber Security Analysis Model that considers the ever changing components of enterprise networks was developed and implemented on windows operating system. Purposive sampling was used to select key informants with technical knowledge about cyber security. Primary data was collected using closed-ended questionnaires and secondary data was collected from analysis of scholarly articles, books, conference papers, and journals. Expert opinion guided the testing and implementation of the developed model.

KEYWORDS: Enterprise networks, Cyber Security, Analysis Model, Dynamic

1. INTRODUCTION

Of recent the use of smart phones, internet and computers is so popular in our lives. This is both for individuals and organizations. As of 2024 there were 5.35 billion internet users worldwide which is 66.2% [1] and according to [2] there are 6.93 billion smartphone users worldwide.

Organizations and enterprises have embraced networking of Computers thus coming up with Enterprise networks. This is attributed to the benefits like resource sharing, remote file storage, and improved communication that come with the networking of computers. However, since access to the server computer affects activities of all computers on the network, cyber-attackers have highly targeted networked computers by exploiting network vulnerabilities thus plunging enterprises into huge financial losses and data losses. Most of the attacks have been as result of errors on the enterprise employees' part.

Cyber-attacks can lead to significant financial losses for large enterprises. The exact amount of losses varies depending on various factors such as the nature of the attack, the size of the organization, the industry sector, and the effectiveness of the organization's security measures. Some notable examples of large enterprises and the losses they have experienced due to cyber-attacks include;

In 2013, Target, a major U.S. retailer, suffered a cyber-attack that compromised payment card information of approximately 40 million customers. The attack also exposed personal information of around 70 million customers. The breach cost Target an estimated $162 million, including expenses related to investigation, remediation, legal fees, and settlements [3].

In 2014, Sony Pictures Entertainment experienced a highly publicized cyber-attack attributed to North Korea. The attack resulted in the theft and release of sensitive company data, including employee information and unreleased films. Sony Pictures estimated the total cost of the attack to be approximately $15 million, including remediation efforts, investigation, and legal fees [4].

In 2017, Equifax, one of the largest credit reporting agencies, experienced a massive data breach that exposed personal information of approximately 147 million people. The breach resulted in significant

financial losses for Equifax, including legal settlements, remediation costs, and damage to its reputation. The estimated total cost of the breach exceeded $1.4 billion [5].

In 2017, Maersk, a global shipping company fell victim to the NotPetya ransomware attack, which affected its IT infrastructure worldwide. The attack resulted in significant disruptions to Maersk's operations, including the shutdown of critical systems and the loss of data. The company reported losses of around $300 million due to the incident [6].

According to the Police Crime report for 2020, Shs. 15 billion was lost through cyber fraud. According to NITA-U, the fraud mostly targeted mobile money and bank operated internet services [7].

It's important to note that these are just a few examples, and the financial impact of cyber-attacks on large enterprises can vary widely. Additionally, the true cost of a cyber-attack may extend beyond immediate financial losses, including reputational damage, customer loss, and regulatory fines.

In a bid to mitigate such attacks enterprises have employed solutions like basic cyber security trainings for all employees, password rotations, 2 factor authentication, and password security policies but in vain.

Due to an increase in situations like cyber-attacks, civil and criminal proceedings, and other industry events, process models were presented and created [8] to address the challenge of Enterprise Network Cyber Security vulnerabilities for example Attack Tree model [9], Attack Graph model [10], STRIDE model and many others. However, the limitation to these models and the aforementioned enterprise solutions is that they work for static networks yet most of the enterprise networks currently are dynamic i.e. the load on the network changes over time, packets to be route come and go, objects in an application are added and deleted constantly, more workstations are constantly added to the network with the increase in the number of employees.

According to [11], the graphical security model-based analysis which would offer a fair solution has several problems that need to be addressed and future research in the areas of adaptability, scalability, and lack of empirical data is suggested. This renders the existing enterprise network security models ineffective.

With such prolific increase in malware attacks targeting Enterprise Networks due to presence of many network vulnerabilities in them which are exploited by cyber-attackers, there is a need to have an Enterprise Network with up-to-date cyber security risk countermeasures. Therefore the major contribution of this study is to develop a Cyber Security Analysis Model that caters for dynamic networks.

2. METHODOLOGY

The methodology that was applied in this research is Design Science Research (DSR). This is due to the fact that DSR is a commonly used and recognized method of producing artifacts in the field of information systems research. It provides a methodical framework for creating objects like constructs, models, procedures, or instances. As a result, it is suitable for designing a DENCAM. DSR is also useful for identifying and implementing feasible solutions within a challenging context [12].

In designing a DENCAM, the following six (6) steps of DSR were followed:

Step 1: Identify the problem and Motivate.

There is an increase in Enterprise networks as a result of several attacks targeting Enterprise Network Systems. Therefore there is need to increase security of the Enterprise Networks such that they are more resistant to such attacks.

Step 2: Define the Objectives

To analyze the security of Enterprise Networks.

To enhance the security of Enterprise Networks.

To simulate several attacks on enterprise networks and observe how the networks counteract them.

Step 3: Design and Development

SolarWinds ipMonitor network monitoring tool was used to monitor the changes in the network components. The new changes in the network components were noted.

MITRE ATT & CK matrix was used as a knowledge base to identify cyber threats to the network and mitigate them. More emphasis was put on the new changes on the network.

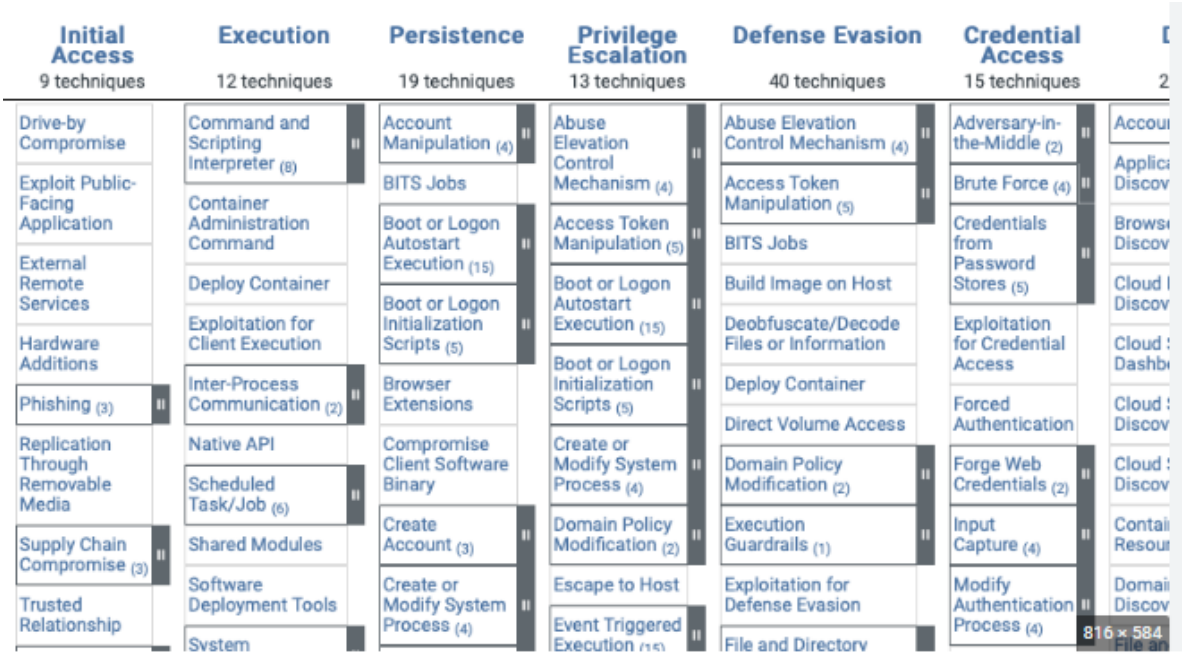


Fig.1. *MITRE ATT & CK matrix*

Step 4: Demonstration
Simulation attacks were launched on the enterprise network using Cymulate threat emulator.
Step 5: Evaluation
The response to the attacks by the Enterprise Network was noted and the Enterprise Network observed to see whether it has behaved as expected.
Mitigations to the Enterprise Network security were put in place for instance security settings of the system will be enhanced to combat such threats in the future.
Step 6: Communication
The research findings were communicated through publishing them.
2.1. Study Area and Period. The study was carried out in Eastern and Central Uganda in the districts of Wakiso, Jinja, Mukono, Buikwe, Iganga, Luuka, and Busia. The study was carried out for a period of 16 months from September 2022 to December 2023.
2.2. Sampling Strategy and Sample. Purposive sampling strategy was used on 56 respondents from 10 enterprises with Enterprise Networks. This is because the required data had to be got from specific Enterprise Network stake holders. In the sample enterprises, Enterprise Managers, Enterprise Network administrators, Enterprise Network users, and Enterprise technicians were targeted.
2.3. *Data Collection Methods*. Survey using semi-structured questionnaires were used to gather data about Enterprise Network stakeholders, and the Enterprise Networks themselves. This is because such questionnaires allow respondents to give detailed responses and also cater for the varying levels of expertise of the respondents. Experimentation data collection method was used to demonstrate the readiness of the Enterprise Networks to combat cyber threats.
2.4. *Data Analysis and Presentations*. Qualitative data was analyzed using Qualitative Content Analysis method because it evaluates patterns within a certain piece of data; and also can be used to identify the frequency with which an idea is shared by the respondents. Quantitative data was analyzed using SPSS tool because it can be used to identify trends, develop predictive models, and also to draw informed conclusions.

2.5. Ethical Consideration. Informed consent; the selected respondents and study population were informed of the study and gave their consent before the study commenced. Voluntary participation; participants in the study voluntarily accepted to participate in the study without coercion or duress. Do not harm; the study and the outcomes of the study were designed in a way that they do not harm the study population. Confidentiality; sensitive information about the sample population was and will never be revealed. Anonymity; the identities of the respondents and sample enterprises were concealed.

2.6. Environmental and Gender implications. This study had minimal negative impact on the environment since the survey questionnaires used were collected after the study for recycling. Also at the end of the study a tree was planted at each of the sample enterprises to help reduce on the carbon dioxide content in the atmosphere. Gender equality and equity was a major determinant in selecting respondents in this study.

2.7. Model Development

2.7.1. Steps in the model. The process of developing the model starts by checking whether the device being analyzed is powered on. If the device is not powered on, then it should be powered on. Once it is confirmed that the device is powered on, it is then checked for network connectivity. The device should be networked if not, then it should be connected to a network. Not just any network but the network of the enterprise in which the device belongs. SolarWinds ipMonitor (Network monitoring tool) is then run to start monitoring the Enterprise Network for changes in its components. Once there are changes, the anomalies and threats are detected MITRE ATT & CK provides the required up-to-date threat knowledge. Lastly, incident Response is immediately implemented as shown in figure 2 below.

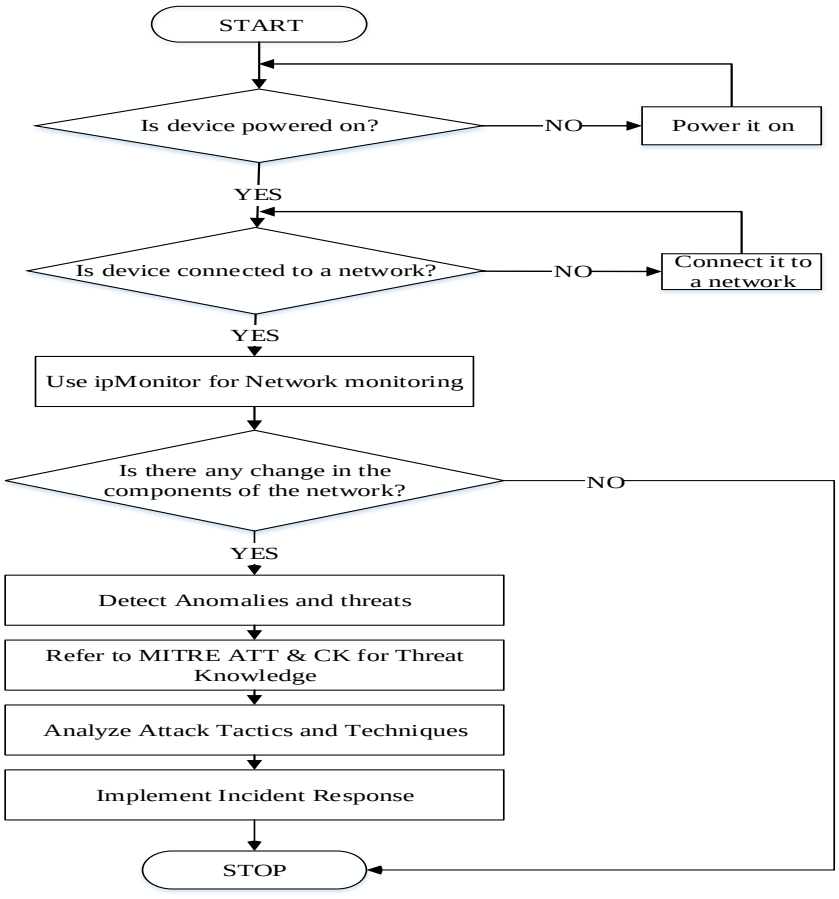


Fig.2. *Dynamic Enterprise Network Cyber Security Analysis Model*

2.8.2. Experimentation. The device being analyzed for Cyber Security threats was powered on and it was ascertained that it was connected to its Enterprise Network. SolarWinds ipMonitor network monitoring tool was used to determine the changes in the components of the network. The interface Solarwinds ipMonitor was as shown in figure 4 below.

3. RESULTS AND DISCUSSION

3.1. Demographic Characteristics. 67 questionnaires were sent to the field of study, however, only 56 were returned fully answered representing a response rate of 83.58%. 58.9% males and 41.1% females responded to the survey; 39.3% of the respondents are in the age bracket of 20 – 39 years while 1.8% in the age bracket of 50 – 59 years. Most of the respondents were from government enterprises representing 62.5% and the remaining 37.5% from private enterprises. 67.9% of the respondents have university degrees while 1.8% have certificates.

3.2. Validity Test. Content Validity Test was used to determine the validity of the questionnaire. Experts were consulted and on examining the tools agreed that 80% of the questions raised can help achieve the objectives of the study. In order to examine the validity on each of the constructs rated against Enterprise Network Cyber Security factor analysis, Principal Component Analysis with varimax rotations was used and the results for each construct were desired and satisfied the analysis as shown in tables 2, 2, and 3 below. KMO was used to determine whether the responses given by the sample are adequate or not. 0.5 is the recommended minimum (barely accepted) KMO value [13]. All responses satisfied this condition as shown in tables 4, 5, and 6.

Tab.1. *Component Factor Loading on the construct of Vulnerabilities*

Component Matrix[a]

	Component 1
Availability of a formal incident response plan	.747
Biggest Cyber Security challenges for the organization	.747

Extraction Method: Principal Component Analysis.

a. 1 components extracted.

Tab.2. *Component Factor Loading on the construct of Threat* Intelligence and Detection

Component Matrix[a]

	Component 1
Ways of Handling Security incidents/breaches	.902

Frequency of vulnerability assessment testing	.902

Extraction Method: Principal Component Analysis.

a. 1 components extracted.

Tab.3. *Component Factor Loading on the construct of Security Controls*

Component Matrix[a]

	Component 1
Rating of organization's network security measures	.831
Number of times security awareness training is conducted	.724
Source of latest Cyber Security threats and trends	.634
Security measures in place	.385

Extraction Method: Principal Component Analysis.

a. 1 components extracted.

Tab.4. *KMO value for Vulnerabilities*

KMO and Bartlett's Test for Vulnerabilities

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.500
Bartlett's Test of Sphericity	Approx. Chi-Square	.715
	df	1
	Sig.	.398

Tab.5. *KMO value for Threat Intelligence and Detection*

KMO and Bartlett's Test for Threat Intelligence and Detection

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.500
Bartlett's Test of Sphericity	Approx. Chi-Square	26.935
	df	1

	Sig.	.000

Tab.6. *KMO value for Security Controls*

KMO and Bartlett's Test for Security Controls

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.582
Bartlett's Test of Sphericity	Approx. Chi-Square	23.334
	df	6
	Sig.	.001

3.3. Reliability Testing. According to [14], reliability is the extent to which a questionnaire provides consistent results. That is to say the ability of a questionnaire to obtain true information. The questionnaires were pre-tested using a small sample population which was not included in the study. Test-retest reliability test was used to determine the consistence of the questionnaire. Cronbach's Alpha test for internal consistence was used on each item of the instrument. Cronbach's Alpha value of 0.653 was obtained which according to [15] is moderate reliability thus making the items of the instrument consistent.

Tab.7. *Reliability statistics*

Reliability Statistics

Cronbach's Alpha	N of Items
.653	16

3.4. SWOT Analysis. The SWOT analysis was done by analyzing related literature about Enterprise Network Cyber threat models and comparing the developed model with the existing models. Table 8 below shows the results from the comparisons.

Tab.8. *Comparison of the developed (DENCAM) with the existing models*

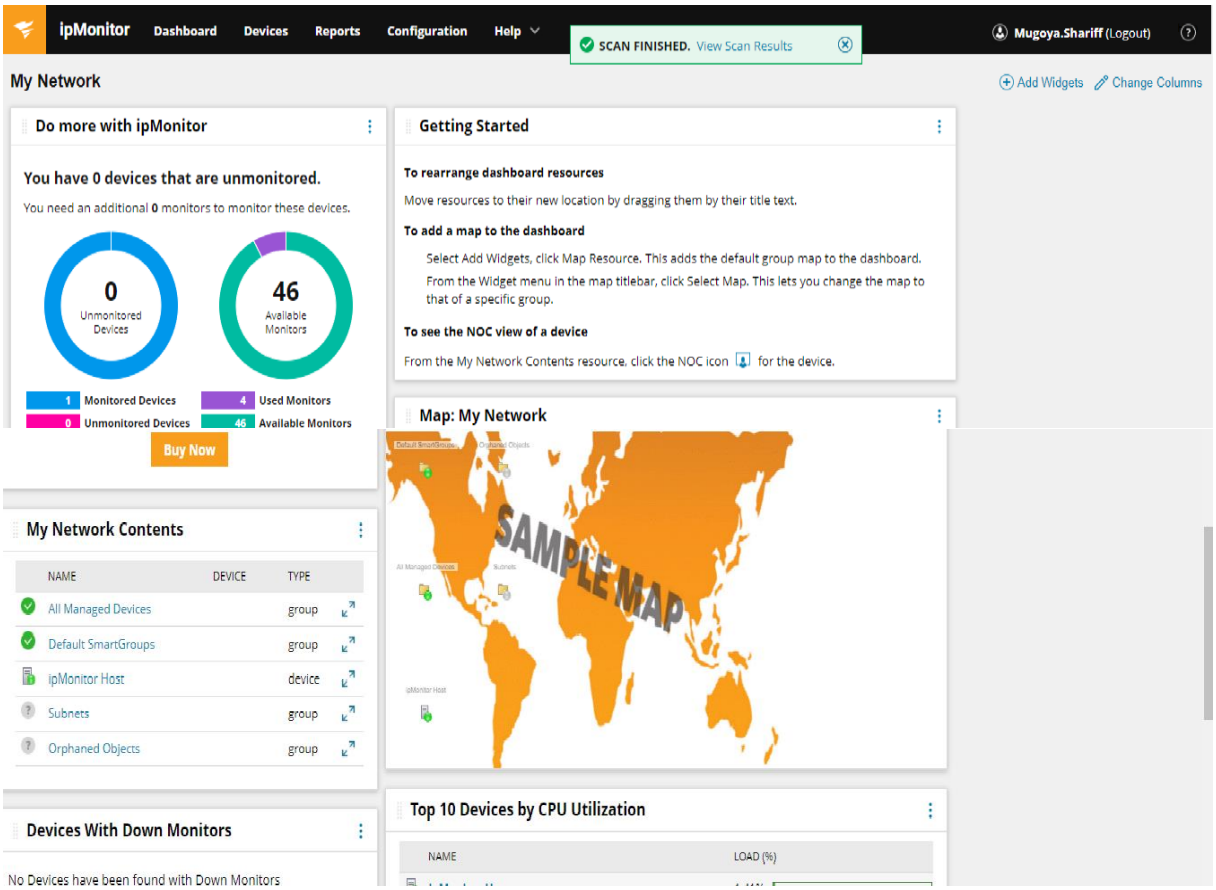
Model	Ability to detect new threats	No false positives	Caters for scalable networks	Caters for Dynamic networks
Signature-based detection	X	X	X	X
Anomaly-based detection	✓	X	X	X
Behavior-based detection	✓	X	✓	X
Machine learning-based detection	✓	X	X	X
Intrusion Detection Systems (IDS)	X	X	X	X
Intrusion Prevention	✓	X	X	X

Systems (IPS)				
Network Traffic Analysis (NTA)	✓	X	X	X
Security Information and Event Management (SIEM)	X	X	✓	X
Threat Intelligence Platforms	✓	X	✓	X
User and Entity Behavior Analytics (UEBA)	✓	X	✓	X

3.5. Experimentation

The device being analyzed for Cyber Security threats was powered on and it was ascertained that it was connected to its Enterprise Network.

SolarWinds ipMonitor network monitoring tool was used to determine the changes in the components of the network. The interface Solarwinds ipMonitor was as shown in figure 3 below.



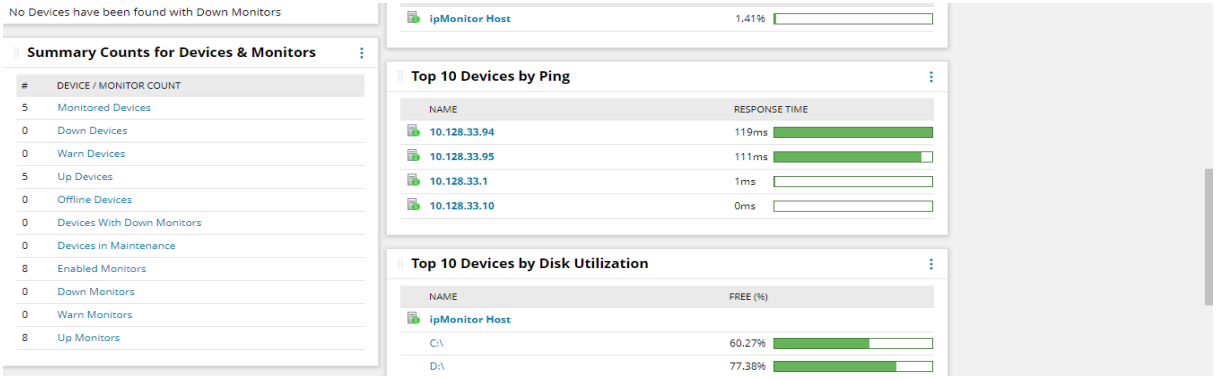


Fig. 3: *Beginning interface of SolarWinds ipMonitor*

Cymulate threat operator was used for simulation attacks. The SolarWinds ipMonitor scanned all the devices in the Enterprise Network and the results were as shown in figure 4 below.

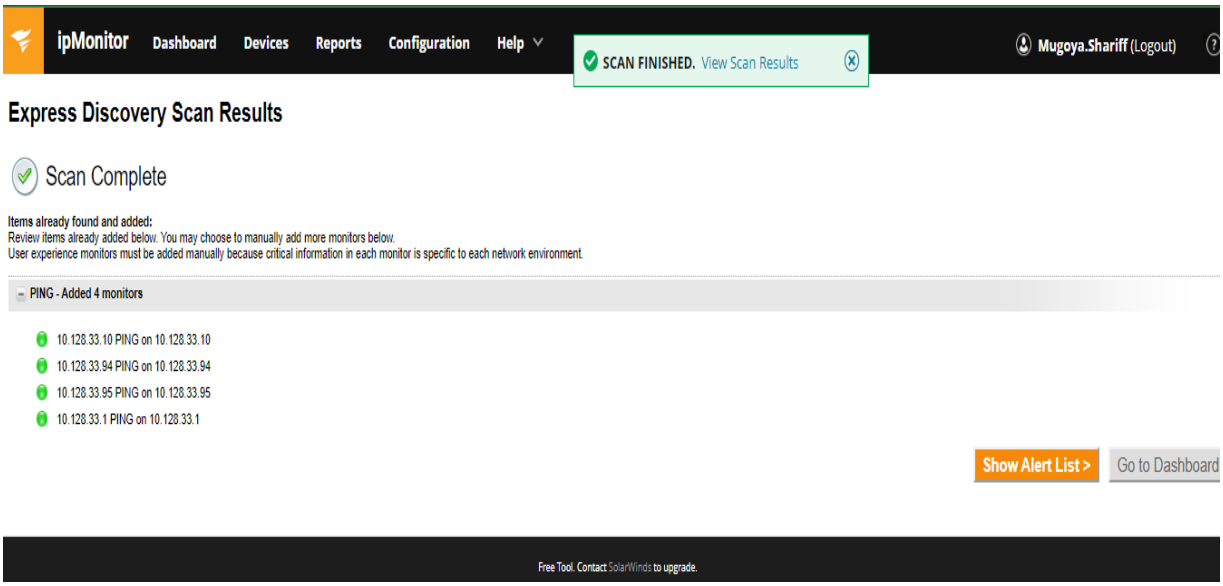


Fig. 0: *Results of Scan*

4 monitors were added to the network making it a total of 46 monitors in the Enterprise Network as shown in figure 4 above.

Scan results for each of the devices in the enterprise Network were as shown in figure 5 below.

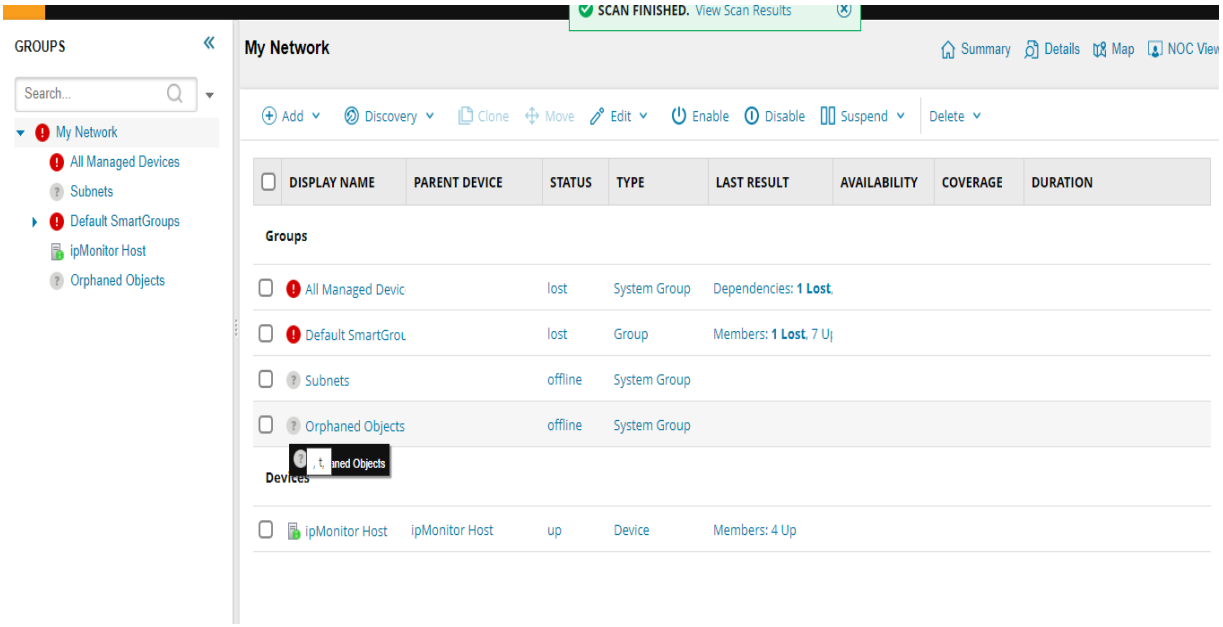


Fig. 5: *Scan Results for the whole network*

The scan results for the Host device was as shown in figure 6 below.

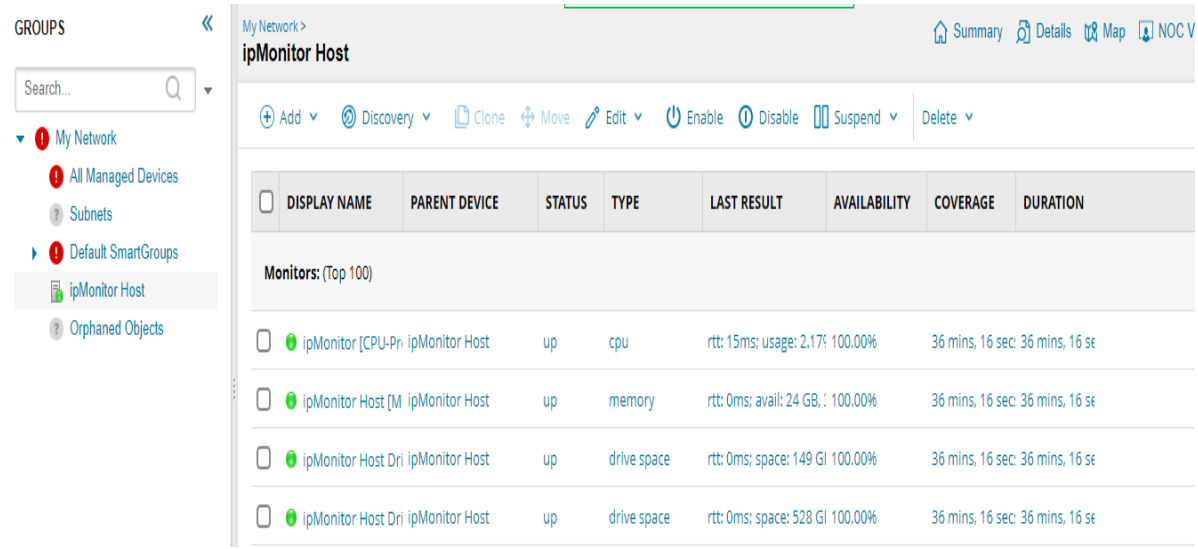


Fig. 6: *Scan Results for Host device*

Report from the scan of the whole network for changes in its components were given as shown in figure 7 below.

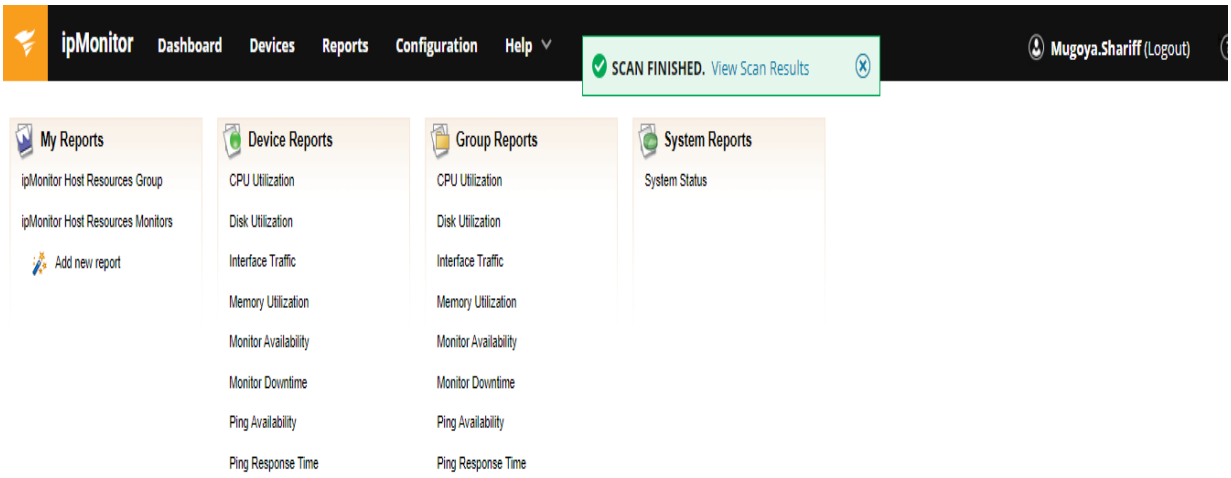


Fig. 7: *Scan Report for the Enterprise Network*

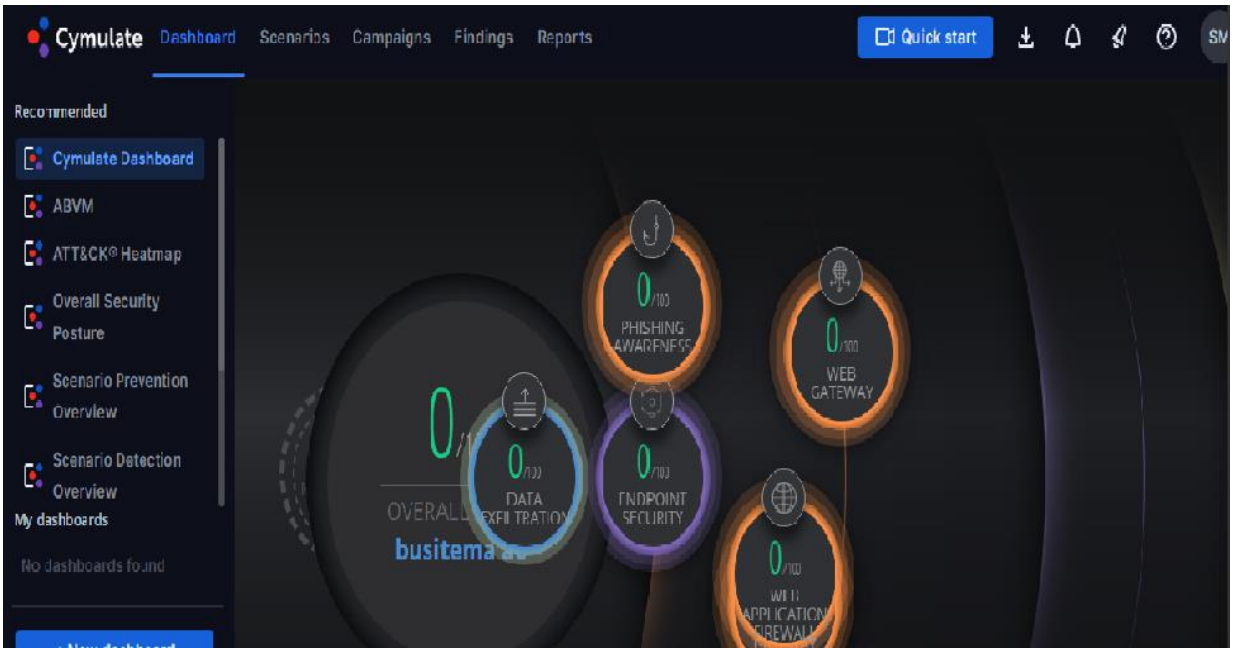


Fig. 8: *Cymulate dashboard*

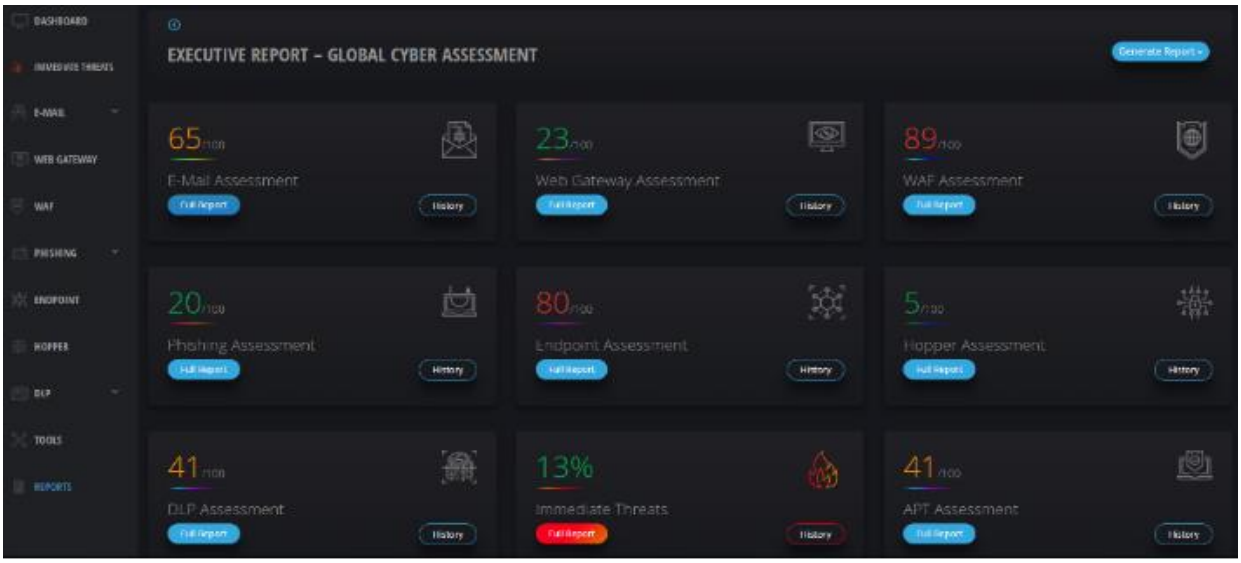


Fig. 9: *Cymulate Simulation report*

4. CONCLUSION AND RECOMMENDATIONS

In this study, an Enterprise Network Cyber Security Analysis Model that considers the constant changes that occur in the components of the network (DENCAM) has been developed. It uses network monitoring tools (e.g. SolarWinds ipMonitor) to monitor the changes in the components of the network, then uses MITRE ATT & CK as a knowledge base for the latest cyber threats and how to combat them. The Incident Response recommended by MITRE ATT & CK is then implemented. The model was tested and validated through experimentation.

Future research should focus on developing a model that can be applied on all operating systems besides Windows operating system.

REFERENCES

1. Statista. (2024). Internet user population. Retrieved from https://www.statista.com/statistics/617136/digital-population-worldwide/ Accessed on January 16th, 2024, at 4:30 P.M.
2. HOW MANY SMARTPHONES ARE IN THE WORLD? (2024). Retrieved from https://www.bankmycell.com/blog/how-many-phones-are-in-the-world. Accessed on January 17th, 2024, at 8: 16 A.M.
3. M. McGrath (2014). Target Data Breach Spilled Info On As Many As 70 Million Customers. Retrieved from https://www.forbes.com/sites/maggiemcgrath/2014/01/10/target-data-breach-spilled-info-on-as-many-as-70-million-customers/?sh=df3f7cce7954. Accessed on January 17th, 2024, at 8:29 A.M.
4. A. DeSimone, and N. Horton. (2015). Sony's Nightmare Before Christmas.
5. M. Hill (2023). The biggest data breach fines, penalties, and settlements so far. Retrieved from https://www.csoonline.com/article/567531/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html. Accessed on January 17th, 2024, at 8:46 A.M.

6. M. Mcquade. (2018). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. Retrieved from https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ Accessed on January 17th, 2024, at 8:52 A.M.
7. Uganda Police Force. (2022). Annual Crime Report. Retrieved from https://www.upf.go.ug/
8. Ocen, G. G., et al. (2019). An Algorithm and Process Flow Model for Extracting Digital Forensic Evidence in Android Devices. International Scientific Journal Theoretical and Applied Science, 72(Issue 04).
9. Schrenier, B. (1999). "Attack trees." Dr. Dobb's Journal, 24(12), 21-29.
10. Phillips, C., & Swiler, L. P. (1998). A graph-based system for network vulnerability analysis (pp. 71-18).
11. S. Yusuf Enoch et al. (2021). Model-based Cyber Security Analysis: Past Work and Future Directions.
12. Bevan , J. L. , Tidgewell , K. D. , Bardull , K. C. , Cusanelli , L. , Hartsern , M. , et al. . (2007). Serial argumentation goals and their relationships with perceived resolvability and choice of conflict tactics.
13. H.F. Kaiser. (1974). An Index of Factorial Simplicity.
14. C.R. Kothari. (2004). Research Methodology: Methods and Techniques.
15. C. B. Perry R, Hinton, Isabella McMurray. (2014). SPSS Explained Second Edition.