(20xx), **x**, 1–8
doi:

ARTICLE

System and Method for AI Based Cyber Hygiene

First Author,[*,1] Second Author,[2] and Third Author[3,1]

[1]Institution-1, City, Country
[2]Institution-2, City, Country
[3]Institution-3, City, Country
*Corresponding author: ankurgupta@mietjammu.in,2020a1r040@mietjammu.in

(Received ; revised ; accepted ; first published online)
(Editor: ; open reviewed by:)

Abstract

The increasing frequency and severity of cyber attacks have made cyber hygiene a critical concern for individuals, organizations, and governments. This review paper examines the different approaches to system and method for cyber hygiene, including policy-based approaches, training and education, and technical solutions. The advantages and disadvantages of each approach are analyzed, with a focus on striking a balance between security and usability. The paper concludes that the most effective cyber hygiene systems , methods and SIEMs will likely combine elements of all three approaches, and provides recommendations for future research in the field. Overall, the paper highlights the importance of cyber hygiene in protecting against cyber threats and emphasizes the need for a comprehensive approach to cyber hygiene that addresses both technical and human factors.

Keywords: Cyber Hygiene , Policy-based approcahes

Abbreviations: SIEM : Security Incident and Event Management

1. Introduction

The paper discusses the challenges of securing information in today's world, where the widespread use of information and communication technology has transformed how businesses operate and employees perform their duties. Cybercriminals are increasingly targeting the human factor in information security, and despite efforts to improve "cyber hygiene," the term is not well understood and its associated practices vary and contradict each other. The article highlights that cybersecurity practices are not always followed even when employees are trained and aware of the risks.

Data privacy and security are critical security measures for any organization. Cybercriminals target personal information on social media, and employees working from home have unlimited access to their organizations' resources, which puts the organizations' data, employees' personal information, and intellectual property at risk. Humans are the weakest link in cybersecurity, and ideally, users would have good cyber hygiene, which means regularly updating software and creating different passwords. However, many users have bad cyber hygiene and do not understand the basics of cybersecurity, which makes them vulnerable to cyber attacks. Small businesses are especially at risk of fraud since they lack security expertise and budget to invest in cybersecurity.

The article notes that research in cybersecurity focuses on improving cyber hygiene behaviour. The factors of cyber hygiene behaviour and the relationship between these factors and cyber hygiene

are identified and analyzed in the article. The authors of the study aim to fill the research gap by recognizing the factors of cyber hygiene behaviour among software engineers and help apply effective cyber hygiene practices.

In conclusion, the article emphasizes the importance of cyber hygiene and the need to change employee behaviour and raise awareness of cyber hygiene practices to protect information resources. Users need more knowledge to improve cybersecurity and change their behaviour, and organizations should provide effective training to all users.

2. Method

2.1 Method and system for evaluating individual and group cyber threat awareness

The system for evaluating the cybersecurity awareness of an organization. This system includes an evaluation server, databases of cybersecurity awareness evaluations, and clients connected to the server. Each client includes a processor, memory, and display and is configured to present cybersecurity awareness evaluations to users of the organization. These evaluations consist of predetermined offensive and defensive actions to attack a competitor's virtual data assets and protect the user's own virtual data assets. The users input their choices of actions and the server generates scoring results based on their inputs.

The evaluation dashboard displays various scores, including offensive and defensive component scores, composite offensive and defensive scores, and risk mitigation scores. The system is further configured to determine and display various other scores, such as a defensive component score for all defensive actions, a composite behavior score, a total risk mitigation score, and a kill chain alignment score. It also calculates a defensive awareness score.

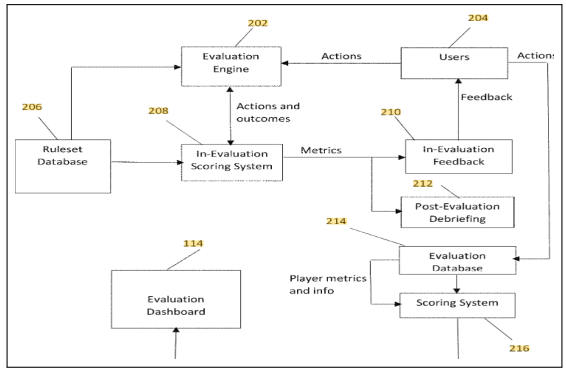

Figure 1. a system architecture overview illustrating the server, database, evaluation dashboard and clients in accordance with embodiments of the invention.

The system aims to provide an effective way of evaluating the cybersecurity awareness of an organization, helping identify areas of improvement and risk mitigation strategies. The system is flexible and configurable, allowing organizations to customize the evaluations based on their specific needs and requirements.

$$BAll - i = \frac{DefAll_i}{P_{Ave}} + \frac{OffAll_i}{\Omega_{Ave}} \tag{1}$$

In this equation, BAll-i represents the composite behavior score for a particular user i, DefAll-i represents the defensive component score for all defensive actions of that user, P-Ave represents

the average scoring weight for defensive actions, OffAll-i represents the offensive component score for all offensive actions of that user, and -Ave represents the average scoring weight for offensive actions.

The equation indicates that the composite behavior score is calculated by dividing the defensive component score by the average scoring weight for defensive actions and adding it to the offensive component score divided by the average scoring weight for offensive actions. This score can help evaluate the overall cybersecurity awareness of a user and identify areas for improvement in defensive and offensive strategies.

2.2 User entity behavioral analysis for preventative attack surface reduction

The method describes a computer device for reducing computer security threats in a network. The method involves monitoring the usage behavior of computer devices in the network, grouping them into clusters based on their usage behavior, and identifying attack surface reduction (ASR) parameters for each cluster. The ASR parameters represent one or more capabilities of the computer devices that can be selectively disabled to improve their cyber security profile. The method involves disabling the identified capabilities based on the ASR parameters.

The grouping of computer devices is done based on their usage behavior during a monitoring time period, which may include applications or services that the computer devices have previously executed or nonuse applications that they have failed to execute. The method includes regrouping the computer devices upon request from a device that needs a disabled capability to be enabled. The method also involves periodically reviewing machine behavior in the clusters and modifying the applied ASR parameters to improve overall cyber hygiene and cluster productivity.

The computer device for reducing computer security threats includes a memory and a processor for executing the instructions to perform the method. The instructions involve monitoring usage behavior, grouping computer devices into clusters, identifying ASR parameters for each cluster, and disabling capabilities of the computer devices based on the ASR parameters. The instructions also involve regrouping computer devices and periodically reviewing machine behavior and ASR parameters.

Overall, the method and computer device aim to improve the cyber security profile of computer devices in a network by selectively disabling capabilities based on ASR parameters and periodically reviewing and modifying them to improve overall cyber hygiene and productivity.

we can represent the process of grouping computer devices in clusters based on their usage behavior using the following equation:

$$C_i = d_j \in D; |; \text{usage}(d_j) \in U_i \tag{2}$$

In this equation, D represents the set of all computer devices in the network, usage(d-j) represents the usage behavior of device d-j, and U-i represents a set of usage behavior patterns that define cluster C-i. The equation says that cluster C-i consists of all devices d-j whose usage behavior matches the pattern set U-i.

We can also represent the process of identifying attack surface reduction (ASR) parameters for each cluster using the following equation:

$$P_i = p_k \in P; |; \text{match}(p_k, C_i) = \text{True} \tag{3}$$

In this equation, P represents the set of all possible ASR parameters, and match(p-k, C-i) represents a function that evaluates whether parameter p-k is appropriate for cluster C-i. The equation says that the set of ASR parameters for cluster C-i is the subset of all possible parameters P that match the characteristics of the devices in cluster C-i.

3.

2.3 Threat evaluation system and method

The text delves into the topic of evaluating the vulnerability of communication network-connected elements to unauthorized access. The methods used by subject matter experts for this evaluation are discussed, with the two main approaches being penetration tests and deterministic models of networks. Penetration tests involve testing the security of a network by attempting to breach it using various methods. Deterministic models of networks involve creating a model of a network and analyzing its security based on the model's assumptions.

However, both these methods have their limitations, such as limited evaluation points, inability to account for changes in network dynamics, and limited methods for attack considered. Therefore, the text suggests a more qualitative approach where a subject matter expert evaluates the threats to a particular target found in a network. This approach involves assessing the security of the services from the target working outward and identifying potential weaknesses. However, this approach is time-intensive and limited to threats known to the evaluator.

The text also emphasizes the complexities involved in quantitatively examining all possible opponent-traversal combinations and states that a tool is required to sort, prioritize, and re-analyze scenarios to produce quantitative results. This tool is a system and method that evaluates threats to the elements of a client computer application. The system comprises a cyber reference library, an opponent catalog, and a network model, and uses a threat evaluation engine, a statistical analysis engine, and analysis results data store to evaluate threats and produce analyst reports.

The text also highlights the importance of accurately identifying and examining all possible threat types, including opponent-traversal, unauthorized access, expected or unexpected state changes, and zero-day vulnerabilities. It stresses the importance of comparing the comprehensive threat profile against existing best practices and system administration procedures, taking into account high-value targets related to business-specific threats regarding security, confidentiality, and trade secrets.

In summary, the text explores the methods and complexities involved in evaluating the vulnerability of communication network-connected elements to unauthorized access. It highlights the limitations of existing methods and the importance of accurately identifying and examining all possible threat types. The present invention is a system and method that aims to address these limitations and produce accurate and quantitative results. Technical terms used in the text include penetration tests, deterministic models of networks, cyber reference library, opponent catalog, threat evaluation engine, statistical analysis engine, and zero-day vulnerabilities.

According to embodiments of the invention, FIG. 1 depicts a high-level system architecture diagram. In some embodiments, the system includes a client application 106 that is connected to a threat evaluation system 104. This evaluation system generates a set of analyst reports 102 that present calculation results to the user. The evaluation system is further linked to a cyber-reference library 108, opponent catalog 110, and network model datastore 112.

There are various ways to establish a communication link between the client application 106 and the threat evaluation system 104, cyber-reference library 108, opponent catalog 110, and network model datastore 112. For instance, a wired or wireless network can connect the threat evaluation system 104 to the cyber-reference library 108. Alternatively, the cyber-reference library 108 may reside on

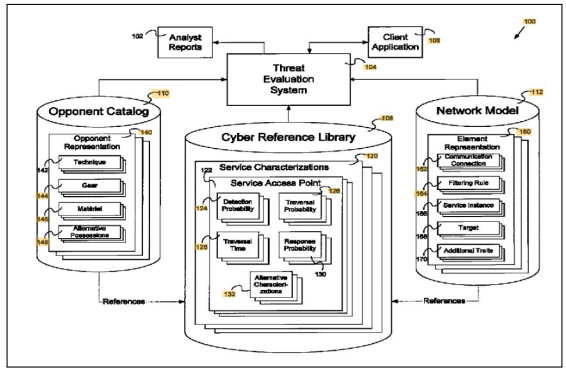

Figure 2. FIG is a top-level diagram of a system architecture according to embodiments of the invention;

the same system as the threat evaluation system 104, in which case interprocess communications mechanisms can be employed. Additionally, the threat evaluation system 104 can communicate with the cyber-reference library 108 over the internet. The embodiments of the invention are not limited to any specific method of connecting the various components.

3. Discussions

Cyber hygiene is an essential aspect of modern-day security that ensures the proper protection of individuals, groups, and organizations from potential cyber threats. This review paper focuses on exploring various systems and methods employed to achieve cyber hygiene, including but not limited to the following:

One method discussed in this paper is the "Method and system for evaluating individual and group cyber threat awareness," which aims to assess an individual's and group's knowledge of cyber threats and how to prevent them. This system provides an efficient way to educate and inform users about the risks associated with cyber threats and how to protect themselves and their organizations.

Another system discussed is the "User entity behavioral analysis for preventative attack surface reduction," which involves analyzing users' behaviors and activities to identify potential threats before they occur. This system relies on machine learning algorithms and artificial intelligence to detect anomalous behaviors and suspicious activities, which can be used to prevent cyber attacks and reduce an organization's attack surface.

Finally, this paper discusses the "Threat evaluation system and method," which is designed to evaluate the vulnerability of communication network-connected elements to unauthorized access. This system uses a threat evaluation engine, a statistical analysis engine, and analysis results data store to evaluate threats to the client computer application and produce analyst reports. This system can help organizations identify potential vulnerabilities and take appropriate measures to mitigate them.

4. Conclusion

In conclusion, cyber hygiene is critical for maintaining a secure online environment. The various systems and methods discussed in this paper, including the "Method and system for evaluating individual and group cyber threat awareness," "User entity behavioral analysis for preventative attack surface reduction," and "Threat evaluation system and method," provide effective ways to ensure that individuals, groups, and organizations are protected from cyber threats. By utilizing these systems

and methods, organizations can significantly reduce their attack surface and prevent potential cyber attacks.

Appendix 1. Supplementary figures

Appendix 1.0.1 Method and system for evaluating individual and group cyber threat awareness

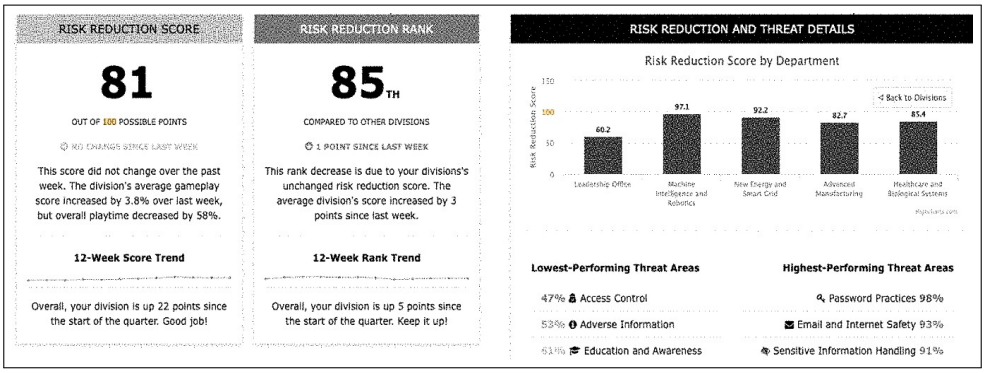

Figure 3. Risk Reduction and Threat Details analysis

Appendix 1.0.2 Threat evaluation system and method

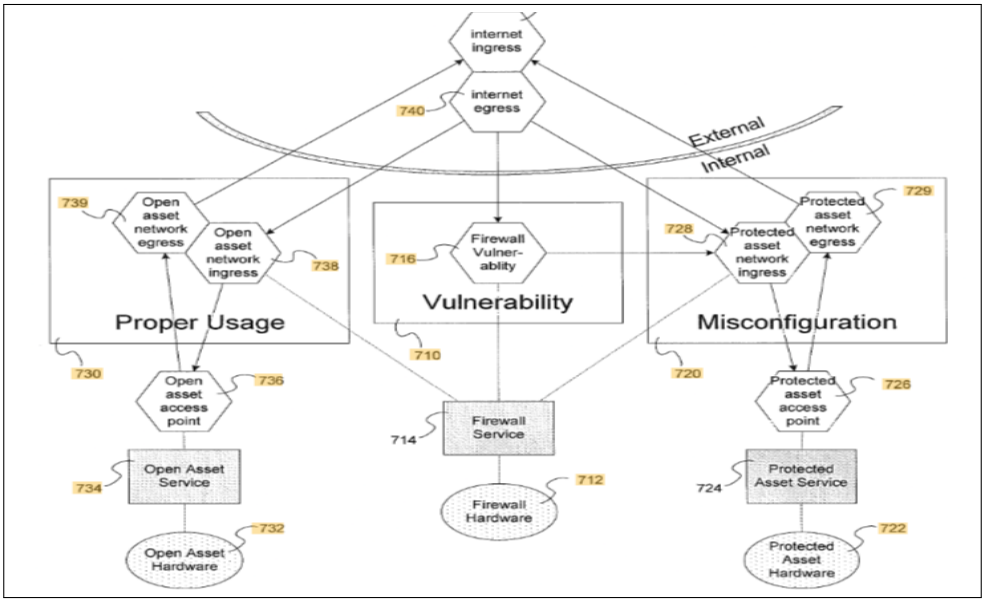

Figure 4. An illustration of the three basic types of service-access point operating on a basic network according to embodiments of the invention;

Appendix 2. Supplementary tables

Appendix 2.0.1 Method and system for evaluating individual and group cyber threat awareness

Metric	Player Value	Player Trend	Department Average	Department Trend	Company Average	Company Trend	Player Percentile
Awareness							
Threat Concepts	89.23		45.33		53.41		90
Risk Mitigation	89.23		45.33		53.41		90
Defensive Strategies	89.23		45.33		53.41		90
Defensive Tactics	89.23		45.33		53.41		90
Conceptual Awareness	89.23		45.33		53.41		90
Applied Awareness	89.23		45.33		53.41		90
Total Awareness	***89.23***		***19.85***		***27.38***		***99th***

Figure 5. A drawing illustrating an evaluation dashboard interface displaying scoring in accordance with embodiments of the invention.

Appendix 2.0.2 Threat evaluation system and method

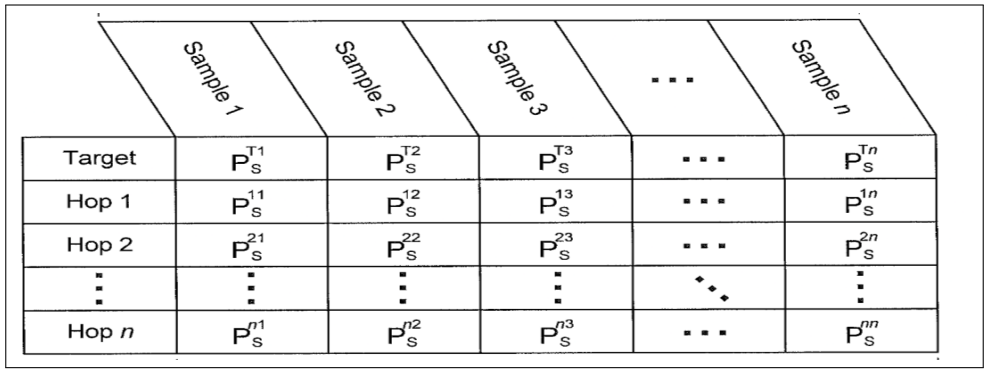

Figure 6. an illustration of an example report provided to analysts using certain embodiments of the invention;

Acknowledgement

Include your acknowledgement in this section.

Author contributions

https://casrai.org/credit/

- First Author: (US11257393B2) Phillip AtencioCassandra BrubakerGeorge A. WrightBrandon DorrisPeter GrundyCharles A. Hardin : Method and system for evaluating individual and group cyber threat awareness : https://patents.google.com/patent/US11257393B2/
- Second Author: (WO2019204062A1) Peter ThayerDeepak Jagannathan ManoharKambiz KouladjieJoseph Carl Nelson BLACKBIRDPrachi RATHEE : User entity behavioral analysis for preventative attack surface reduction : https://patents.google.com/patent/WO2019204062A1/
- Third Author: (US9774616B2) Roderick A. FloresBritny Rolston : Threat evaluation system and method : https://patents.google.com/patent/US9774616B2/en

Funding statement

When applicable, please specify the funding information for this research.

Open data statement

DOI and short description to supplementary data.

Reproducibility statement

Information on how to reproduce this research, including access to 1) source code related the research, 2) source code for the figures, 3) source code / data for the tables when applicable.