Effectiveness of Cyber security early warning and detection systems

Abstract:

Cyber attackers are ramping up their activities with some of the advanced methods that the defenders are slowly upgrading to their correct protection steps. Cybersecurity monitoring should facilitate proactive assistance focused on the relevant preparation as early as possible, with an emphasis on the long-term value in the correct scaling of details. In this segment it is quite appropriate to provide constructive alerts and generate the preliminary assignment criteria to aim for possible solutions. In this research, the respondents' effective information, the literature review, and the specific recommendations help structure the overall research idea. A generic set of information gathering, careful information deployment, and access to the information infusion help to consider the likely direction for managing the security warning. Use real-world scenarios, convincing correct inspiration and offering strategically applied behavioural research help collect the necessary ideas. The early warning and detection system are useful to deal with any current-time intrusion that a traditional intrusion detection system cannot detect. It makes associating with their various projects that require high security from any external cyber threat more trustworthy for both governmental and private organisations.

Introduction:

The criteria for getting and advanced programme are important along with new technologies as the older systems are becoming obsolete and can be ignored by the hackers. The cybersecurity early warning and monitoring programme was built in this phase by taking into account the growing security issues. This is a standalone system and can be incorporated with artificial intelligence to improve its response according to different users needs (mouavinejad et al.2018). The main challenge for safety in the current scenario is to include network protection capabilities in order to address various sources of weaknesses and threats. The current early warning and detection system for cybersecurity is the effective development to address the threats and vulnerabilities that an organisation's IT security team faces generally raises query and asks for fast solutions.

Research questions:

1) Is FIDeS effective solution and possible solution to the development and application of Cybersecurity Early Warning and Detection System?

2) What major threats are to be faced on the implication of Cyber security early warning and Detection system on data protection and stability?
3) What impact do organisations belonging to different industry obtain using Cyber security early warning and detection systems?

Background:

The main security challenge in the current scenario is to include network protection capabilities to address diverse sources of weaknesses and threats. The current cyber security early warning and detection system is the effective development to address the threats and vulnerabilities faced by the IT security team of an organisation. All devices can interact with each other in the coming time, and the user can see it as a single, bounded network in which the total procedure is needed to be secured. A huge amount of data will be stored in cloud systems in the 'Internet of the Future' and for this reason testing, privacy and security will become essential for data storage. The typical protocols might not be necessary in this situation in order to establish appropriate protection for the cloud network that is still linked to the Internet. A proactive security system infrastructure is required, and for this reason the early warning and detection system has been developed that can replace the traditional detection system and provide better security for different organisations around the globe. Cyber offenders conduct analysis which can recognise the efficacy of early alert which monitoring programmes with primary and secondary process.

Methodology:

The given research is to be developed by using qualitative and quantitative research methods that would help in increasing the insights gained on the research data and allow the effective usage of a wide range of resources for the data collection process. The use of qualitative research is based on the effect it can obtain on the data collected by open-ended sources that would further allow the research to be conducted based on non-numerical format pertaining to the development of theoretical analysis. The use of the qualitative research could help in Page 6 of 7 gathering knowledge from the different types of materials that are already present and has been researched on considering the given topic by other researchers following the given research project or obtain an insight on the possible gaps to be fulfilled (Park and Park, 2016). In addition, there would be the use of quantitative research strategy that would gather numerical data that are focused on providing a factual basis for the research process. The research would further allow the effective demonstration and meeting the objectives of the research as it has been developed considering the range of resources that are available to provide with numerical and unbiased data (Brannen, 2017).

Data collection techniques:

The data collection technique that would be taken into account is based on the selection and gathering of both secondary and primary data. It has been noted that the data collection technique that is to be used for secondary data is based on qualitative research to be carried out. This would involve the use of the different types of journals, articles, documents and other research materials, which would help in identifying the potential benefits and negative impacts of issues presented, by the use of cyber

security early warning and detection systems in the companies. In addition, the collection of the primary data would be carried out based on the quantitative research process that is based on using a survey process that would be carried out by twenty security officials working in the information security system located in the given country (Abildgaard et al. 2016). The sampling method to be used for the selection of the security officials is cluster sampling technique to identify the possible security officials and then followed by the use of a simple random sampling technique to select the twenty officials as participants.

References:

1) Petrenko, S.A. and Makoveichuk, K.A., 2017. Big data technologies for cybersecurity. In CEUR Workshop (pp. 107-111).
2) Amsler, D.B., Allen, N., Messer, S. and Healy, T., Rayteon Foreground Security, Inc., 2016. Automated internet threat detection and mitigation system and associated methods.
3) Bahraminejad, M., Rayegani, B., Jahani, A., and Nezami, B., 2018. Proposing an early warning system for optimal management of protected areas (Case study: Darmiyan protected area, Eastern Iran). Journal for Nature Conservation, 46,pp.79-88.
4) Bengtsson, L., Borg, S., and Rhinard, 2018. European security and early warnmg Bengtsson, L., Borg, S., and Rhinard, M., 2018. European security and early warnmg Secwity, 27(1), pp.20-40.
5) Chen, L., Liu, L., Peng, Y., Chen, W., Huang, H., Wu, T. and Xu, X., 2020. Distribution network operational risk assessment and early warning considering multi-risk factors. JET Generation, Transmission & Distribution.
6) Han, X., Kheir, N. and Balzarotti, D., 2017, October. Evaluation of deception-based web In Proceedings of the 2017 Workshop on Moving Target Defence (pp. 65- 73).
7) Vigneswaran, K.R., Vinayakumar, R., Soman and Poornachandran, P., 2018, July. Evaluating shallow and deep neural networks for network intrusion detection systems in cyber security. 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (pp. 1-6). IEEE.
8) Park, J. and Park, M., 2016. Qualitative vs quantitative research methods: Discovery or justification? Journal of Marketing Thought, 3(1), pp.1-8.
9) Karimipour, H., Dehgntanha, A., Parizi, R.M., Choo, K.K.R. and Leung, H., 2019. A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids. *IEEE* Access, 7, pp.80778-80788.
10) Kure, H. and Islam, S., 2019. Cyber Threat Intelligence for Improving Cybersecurity and Risk Management in Critical Infrastructure. Journal of Universal Computer Science, *25(11),* pp.1478-1502.

11) Simatupang, J.W. and Naufal,F., 2019. Flood Early Warning Detection System Prototype Based on IoT Network. Internetworking Indonesia Journal, 11, pp.17-22.
12) Vinayakumar, R., Alazab, M., Soman, Poornachandran, Al-Nemrat,A. and venkatraman, S 2019.