ESCAF 3rd 2024
p-ISSN : 2962 - 7710
e-ISSN : 3021 - 8594

THE IMPORTANCE OF IMPLEMENTING CYBER SECURITY IN IMPROVING DATA SECURITY

Ahmad Sainuri Mubarak[1], Mutahira Nur Insirat[2]
[1]Computer and Network Engineering, SMK Negeri 4 Gowa, South Sulawesi
[2]Departement of Accounting, Muhammadiyah Makassar University, South Sulawesi
e-mail: *[1]ahmadsainurimubarak@gmail.com, [2]mutahiranurinsiratimran932@gmail.com

Abstrak

Tidak dapat dipungkiri bahwa saat ini kehadiran informasi merupakan hal yang cukup signifikan bagi semua perusahaan dan organisasi. Oleh karena itu, melindungi keamanannya sangatlah penting. Dari sudut pandang keamanan ini, keamanan jaringan merupakan masalah yang signifikan karena kapasitas serangan terus meningkat selama bertahun-tahun dan menjadi lebih canggih dan berdistribusi, Keamanan siber, khususnya dalam mencegah serangan eksternal terhadap perangkat keras, perangkat lunak, dan data yang terhubung ke internet, merupakan fokus utama bagi organisasi. Organisasi menerapkan langkah-langkah keamanan siber untuk melindungi basis data dan sistem mereka dari akses yang tidak sah. Berbagai bentuk serangan seperti akses tidak sah, perangkat lunak perusak, kegagalan layanan, pengelabuan tipe rekayasa sosial, serangan *zero-day* dan lain sebagainya menjadi tanggung jawab atas masalah keamanan ini. Penelitian ini menggunakan metode literature review dengan tujuan untuk menganalisis, mengevaluasi, dan mensintesis sumber-sumber literatur yang relevan dengan topik penelitian. Tujuan dari penelitian ini adalah untuk membahas konsep keamanan cyber, keamanan cyber dan risiko keamanan, strategi pertahanan keamanan cyber, serta masalah penelitian dan arah masa depan.

Kata kunci: Keamanan siber, risiko, strategi

Abstract

It cannot be denied that currently the presence of information is quite significant for all companies and organizations. Therefore, protecting its security is very important. From this security perspective, network security is a significant issue as attack capacity has continued to increase over the years and become more sophisticated and distributed, Cybersecurity, particularly in preventing external attacks on internet-connected hardware, software and data, is the main focus for the organization. Organizations implement cybersecurity measures to protect their databases and systems from unauthorized access. Various forms of attacks such asunauthorized access, malware, service failures, social engineering type phishing, zero-day attacks and so onbe responsible for this security issue. This research uses a literature review method with the aim of understandinganalyze, evaluate, and synthesize literature sources relevant to the research topic.The aim of this research is todiscusses cyber security concepts, cyber security and security risks, cyber security defense strategies, as well as research issues and future directions.

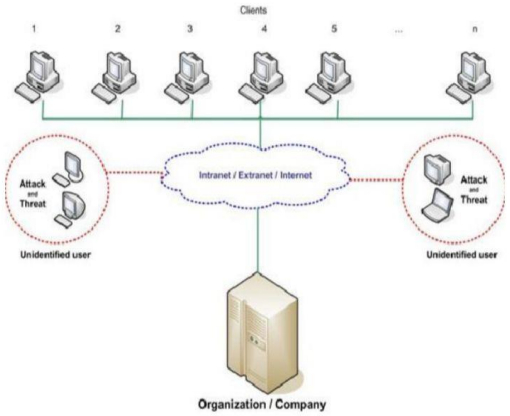
Keywords: *cyber security; risk; strategy*

I. INTRODUCTION

Cybersecurity is a set of security precautions to ensure the confidentiality, integrity and availability of data (Dua & Du, 2016). According to Canongia and Mandarino, cyber security is the art of ensuring the existence and continuity of a nation's information, guaranteeing and protecting cyberspace, information, assets and critical infrastructure.(Canongia & Mandarino, 2012). Cyber security

ESCAF 3rd 2024
p-ISSN : 2962 - 7710
e-ISSN : 3021 - 8594

components consist of network security, application security, mobile security, data security, endpoint security and so on(Twomey, 2010). Over the last few years, the use of the internet and computer applications has experienced a huge expansion and has become an integral part of today's generation. With the increase in computer applications and use of computer networks, security has become very important. Attacks can potentially use multiple paths through an application to wreak havoc on a business or organization. Figure 1 illustrates some potential attacks and threats to organizations.



Source: Canongia & Mandarino (2012)

Figure 1. Potential Attacks and Threats to Organizations

All of these paths represent risks that may be serious enough to require attention. The Financial Services Authority (OJK) noted that based on data from the Institute of Internal Auditors (IIA) losses due to cybercrime worldwide in 2023 will reach 8 trillion US dollars (Reyhan Ghifari, 2023). The increasing percentage of cyber attacks has led to artificial intelligence and machine learning-based methodologies becoming an important part of detecting security threats. For the best security applications to be accepted and the appropriate level of security achieved, security benchmarks are essential. Although there are several studies on specific data sets, there are still few studies that study the comprehensive status of security-related data sets. With the information received data is collected to detect suspicious connections.

In general, there are three methods used to detect cyber attacks. These are signature-based attack detection, anomaly-based attack detection, and hybrid-based attack detection systems. In signature-based detection methods, each attack is recorded by creating a dictionary (word list) with uniquely defined signatures. Every newly detected attack is stored in this dictionary. Thus, a defense system is formed based on known and discovered attacks (Meng et al., 2014)**.** Anomaly detection methods evaluate whether there is an unusual situation or not by extracting information packets from network traffic. If an abnormal situation is detected, then an anomaly detection-based system can detect attacks that cannot be detected by a signature-based detection system. To increase detection success, hybrid systems have been developed by combining these two approaches. In detecting attacks, machine learning techniques provide higher accuracy on network traffic. The research results show that the intrusion detection approach using machine learning algorithms provides higher success when compared to other methods (Meng et al., 2014; Suaib Akhter et al., 2021)**.**

Security risks are usually associated with any attack considering three security factors, such as threat i.e. who is attacking, vulnerability i.e. the weakness being attacked, and impact i.e. what the attack does (Fischer, 2016). A security incident is an action that threatens the confidentiality, integrity, or availability of information assets and systems. Defense strategies are needed to protect data or information, information systems and networks from cyber attacks or intrusions. In more detail, they are responsible for preventing data

ESCAF 3rd 2024
p-ISSN : 2962 - 7710
e-ISSN : 3021 - 8594

breaches or security incidents and monitoring and reacting to intrusions, which can be defined as any type of unauthorized activity that causes damage to information systems (Khraisat et al., 2019). Intrusion detection systems are typically represented as devices or software applications that monitor a network or computer system for malicious activity or policy violations (Johnson, 2013).

The aim of this research is to discusses the concept of cyber security, cyber security and security risks, cyber security defense strategies, as well as research problems and future directions which can later be used as guidelines for future researchers in the field of cyber security.

The second part of this research explains important security concepts, the third part explains cyber security and security risks, the fourth part explains cyber security defense strategies, the fifth part explains research problems and future directions, finally provides a conclusion on what has been presented.

II. RESEARCH METHODS

This research uses a literature review research method. The literature review method is an activity that involves analysis, evaluation and synthesis of literature sources relevant to the research topic.

III. RESULTS AND DISCUSSION

Cyber Security Concept

Over the past half century, the information and communications technology industry has grown rapidly, become ubiquitous and closely integrated with modern society. Therefore, protecting information and communications technology systems and applications from cyber attacks has become a major concern of security policymakers in recent days (Sun et al., 2019). The act of protecting information and communication technology systems from various kinds of cyber threats or attacks is known as cyber security (Fischer, 2016).

Several aspects related to cyber security: measures to protect information and communication technologies; raw data and the information they contain and their processing and transmission; related virtual and physical elements of the system; the level of protection resulting from the implementation of such measures; and related professional business fields (Fischer E, 2005). Craigen et.al defines cyber security as a set of tools, practices and guidelines that can be used to protect computer networks, software programs and data from attack, damage or unauthorized access (Craigen et al., 2014). According to Aftergood et.al (Aftergood, 2017)**,** cyber security is a set of technologies and processes designed to protect computers, networks, programs, and data from attacks and unauthorized access, alteration, or destruction. Overall it can be concluded that cyber security is concerned with understanding various cyber attacks and designing appropriate defense strategies to maintain some of the properties explained below (Jang-Jaccard & Nepal, 2014; Lin et al., 2007)

1. Confidentiality
   It is a property used to prevent access and disclosure of information to unauthorized individuals, entities, or systems.
2. Integrity
   These are properties used to prevent modification or destruction of information in an unauthorized manner.
3. Availability
   Represents property used to ensure timely and reliable access of assets and information systems to authorized entities.

ESCAF 3rd 2024
p-ISSN : 2962 - 7710
e-ISSN : 3021 - 8594

The term cyber security applies in a variety of contexts, from business to mobile computing, and can be divided into several general categories, including:

1. Network security whose main focus is securing computer networks from cyber attackers or intruders.
2. Application security that considers keeping software and devices free from cyber risks or threats.
3. Security information primarily considers the security and privacy of relevant data.
4. Operational security which includes the process of handling and protecting data assets.

Cyber Security and Security Risks

Risk is usually associated with any attack considering three security factors, such as threat i.e. who is attacking, vulnerability i.e. the weakness being attacked, and impact i.e. what the attack does (Fischer, 2016). A security incident is an action that threatens the confidentiality, integrity, or availability of information assets and systems. Several types of cyber security incidents can result in security risks to an organization's or individual's network systems (Sun et al., 2019) as follows.

1. Unauthorized access describes the act of accessing information to a network, system or data without permission resulting in a violation of security policies (Fischer, 2016);
2. Malware. Known as malicious software. This malware is intentionally designed to cause damage to a computer, client, server, or computer network. Examples of various types of malware include computer viruses, worms, adware, ransmoware, spyware, bad bots, and so on (McIntosh et al., 2019). Ransmoware is a form of malware that appears to prevent users from accessing their systems or personal files or devices, then demands anonymous online payments to restore access.
3. A failure of service is an attack intended to shut down a machine or network, making it inaccessible to intended users by flooding the target with crash-inducing traffic (Fischer, 2016).
4. Phishing is a type of social engineering, used for a variety of malicious activities carried out through human interaction, which is a fraudulent attempt to obtain sensitive information such as banking and credit card details, login credentials, or personally identifiable information by impersonating a trusted individual or entity through communications. electronics such as email, text, or instant messages, and so on (Jang-Jaccard & Nepal, 2014).
5. Zero-day attack is considered a term that describes the threat of unknown security vulnerabilities for which patches have not been released or application developers are unaware of (M. Alazab et al., 2011; Bilge & Dumitras, 2012)

In addition, there are several security attacks known as security incidents in the field of cyber security, including privilege escalation (Davi et al., 2010), password attacks (Jovičić & Simić, 2006), insider threats (Warkentin & Willison, 2009), constant threat (Kügler, 2003), web application attacks (Jovičić & Simić, 2006), SQL injection attacks (Boyd & Keromytis, 2004) and so on.

Cyber Security Defense Strategy

Defense strategies are needed to protect data or information, information systems and networks from cyber attacks or

ESCAF 3rd 2024
p-ISSN : 2962 - 7710
e-ISSN : 3021 - 8594

intrusions. In more detail, they are responsible for preventing data breaches or security incidents and monitoring and reacting to intrusions, which can be defined as any type of unauthorized activity that causes damage to information systems (Khraisat et al., 2019). Intrusion detection systems are typically represented as devices or software applications that monitor a network or computer system for malicious activity or policy violations (Johnson, 2013). Well-known traditional security solutions such as anti-virus, firewall, user authentication, access control, data encryption and cryptographic systems, however, may not be effective according to current needs in the cyber industry (Anwar et al., 2017; Mohammadi et al., 2019; Tapiador et al., 2015; Tavallaee et al., 2010). On the other hand, intrusion detection systems can be used to detect internal attacks and external attacks. Intrusion detection systems have different categories according to their scope of use. Based on methodology, intrusion detection systems are divided into:

1. Signature-based intrusion detection system

Signatures can be predefined strings, patterns, or rules that relate to known attacks. Certain patterns are identified as detection related attacks in signature-based intrusion detection systems. Examples of signatures can be known patterns or sequences of bytes in network traffic, or sequences used by malware. To detect such attacks, anti-virus software uses such types of sequences or patterns hence signatures are used when performing matching operations. Signature-based intrusion detection systems are also known as knowledge-based or abuse detection (Liao et al., 2013).This technique is efficient for processing high volumes of network traffic, but being limited to invisible attacks is one of the biggest challenges faced by these signature-based systems.

2. Anomaly-based intrusion detection system

The concept of an anomaly-based intrusion detection system overcomes the problem of signature-based intrusion detection systems. In an anomaly-based intrusion detection system, network behavior is first examined to find dynamic patterns in order to automatically create a data-driven model, to profile normal behavior, and thereby detect deviations in case of anomalies (Liao et al., 2013). Thus, anomaly-based intrusion detection systems can be treated as a dynamic approach, which follows behavior-oriented detection. The main advantage of an anomaly-based intrusion detection system is its ability to identify unknown attacks or zero-day attacks (A. Alazab et al., 2012). However, the problem is that identified anomalies or abnormal behavior are not always indicators of an intrusion. Sometimes this can occur due to several factors such as policy changes or new service offerings.

3. Hybrid detection approach

Hybrid detection approach (Viegas et al., 2017; Xin et al., 2018) that takes into account misuse and the anomaly-based techniques discussed above can be used to detect intrusions. In a hybrid system, the abuse detection system is used to detect known types of intrusions and the anomaly detection system is used for new attack detection (Dutt et al., 2018). In addition to these approaches, stateful protocol analysis can also be used to detect intrusions identifying protocol state deviations similar to anomaly-based methods, however these methods use predefined universal profiles based on accepted benign activity definitions (Liao et al., 2013). Once detection is complete, intrusion prevention systems, which are intended to prevent malicious events, can be used to mitigate

ESCAF 3rd 2024
p-ISSN : 2962 - 7710
e-ISSN : 3021 - 8594

the risk in various ways such as manual, providing notifications, or automated processes (Ragsdale et al., 2000). Among these approaches, automated response systems can be more effective because they do not involve a human interface between detection and response systems.

Research Issues and Future Directions

1. Addressing quality issues in cyber security datasets. Cyber data sets may be problematic such as incomplete, insignificant, unbalanced, or may contain inconsistencies related to specific security incidents. Issues in such datasets can impact the quality of the learning process and degrade the performance of machine learning-based models(Sarker, 2019). To make intelligent data-driven decisions for cyber security solutions, such data problems need to be addressed effectively using novel algorithms proposed for specific problem domains such as malware analysis, or intrusion detection and prevention which can be another research issue in cyber security data science.
2. Creation of security policy rules. Security policy rules refer to security zones and allow users to allow, restrict, and track traffic on a network based on the associated user or user group, and service, or application. Policy rules include general and more specific rules compared to incoming traffic sequentially during execution, and rules that match that traffic are applied. The policy rules used in most cyber security systems are static and generated by human expertise or ontology-based(Kayes et al., 2014, 2018). Although association rule learning techniques generate rules from data, there is a problem of generating redundancy(Sarker & Salim, 2018)which makes policy rules complicated. Therefore, understanding these problems in creating policy rules effectively using existing algorithms or newly proposed algorithms for other research problem domains in cyber security data science.
3. Feature engineering in cyber security
   The efficiency and effectiveness of machine learning-based security models has always been a big challenge due to the high volume of network data with a large number of traffic features. The large dimensions of data have been addressed using several techniques such as principal component analysis(Sarker et al., 2020). In addition to low-level features in the dataset, contextual relationships between suspicious activities may be relevant. This contextual data can be stored in an ontology or taxonomy for further processing. So how to effectively select optimal features to extract important features by considering low-level features as well as contextual features for effective cyber security solutions can be another research issue in cyber security data science.

IV. CONCLUSION

Motivated by the increasing importance of cyber security. So we have discussed cyber security concepts, cyber security and security risks, cyber security defense strategies, and research issues and future directions. Cyber security impacts security data, both in terms of extracting insights about security incidents and related security services. The purpose of this article is to provide an overview of the conceptualization, understanding, modeling, and thinking about cyber security data science. We have identified and further discussed key issues in security analytics to

ESCAF 3rd 2024
p-ISSN : 2962 - 7710
e-ISSN : 3021 - 8594

suggest future research directions in the cyber security data science domain.

V. SUGGESTIONS

To make intelligent data-driven decisions for cyber security solutions, such data problems need to be addressed effectively using novel algorithms proposed for specific problem domains such as malware analysis, or intrusion detection and prevention which can be another research issue in cyber security data science; understanding about creation of security policy rules in creating policy rules effectively using existing algorithms or newly proposed algorithms for other research problem domains in cyber security data science; and effectively select optimal features to extract important features by considering low-level features as well as contextual features for effective cyber security solutions can be another research issue in cyber security data science.

VI. REFERENCES

Aftergood, S. (2017). Cybersecurity: The cold war online. *Nature 2017 547:7661*, *547*(7661), 30–31. https://doi.org/10.1038/547030a

Alazab, A., Hobbs, M., Abawajy, J., & Alazab, M. (2012). Using feature selection for intrusion detection system. *International Symposium on Communications and Information Technologies*, 296–301. https://doi.org/10.1109/ISCIT.2012.6380910

Alazab, M., Venkatraman, S., Watters, P., & Alazab, M. (2011). Zero-day Malware Detection based on Supervised Learning Algorithms of API call Signatures. *Australasian Data Mining Conference*.

Anwar, S., Zain, J. M., Zolkipli, M. F., Inayat, Z., Khan, S., Anthony, B., & Chang, V. (2017). From Intrusion Detection to an Intrusion Response System: Fundamentals, Requirements, and Future Directions. *Algorithms*, *10*(2). https://doi.org/10.3390/A10020039

Bilge, L., & Dumitras, T. (2012). Before we knew it: An empirical study of zero-day attacks in the real world. *Proceedings of the ACM Conference on Computer and Communications Security*, 833–844. https://doi.org/10.1145/2382196.2382284

Boyd, S. W., & Keromytis, A. D. (2004). SQLrand: Preventing SQL injection attacks. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *3089*, 292–302. https://doi.org/10.1007/978-3-540-24852-1_21/COVER

Canongia, C., & Mandarino, R. (2012). Cybersecurity: The New Challenge of the Information Society. *Crisis Management: Concepts, Methodologies, Tools, and Applications*, *1–3*, 60–80. https://doi.org/10.4018/978-1-4666-4707-7.CH003

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, *4*(10), 13–21. https://doi.org/10.22215/TIMREVIEW/835

Davi, L., Dmitrienko, A., Sadeghi, A. R., & Winandy, M. (2010). Privilege Escalation Attacks on Android. *Information Security Conference*, *6531 LNCS*, 346–360. https://doi.org/10.1007/978-3-642-18178-8_30

Dua, S., & Du, X. (2016). Data Mining and Machine Learning in Cybersecurity. *Data Mining and Machine Learning in Cybersecurity*. https://doi.org/10.1201/B10867

Dutt, I., Borah, S., Maitra, I. K., Bhowmik, K., Maity, A., & Das, S. (2018). Real-Time Hybrid Intrusion Detection System Using Machine Learning Techniques. *Lecture Notes in Electrical Engineering*, *462*, 885–894. https://doi.org/10.1007/978-981-10-7901-6_95/COVER

Fischer E. (2005). *Creating a National Framework for Cybersecurity: An Analysis of Issues and Options*. https://www.researchgate.net/publication/235122081_Creating_a_National_Framework_for_Cybersecurity_An_Analysis_of_Issues_and_Options

Fischer, E. A. (2016). *Cybersecurity Issues and Challenges: In Brief*. www.crs.gov

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973–993. https://doi.org/10.1016/J.JCSS.2014.02.005

ESCAF 3rd 2024
p-ISSN : 2962 - 7710
e-ISSN : 3021 - 8594

Johnson, L. R. (2013). Computer Incident Response and Forensics Team Management: Conducting a Successful Incident Response. *Computer Incident Response and Forensics Team Management: Conducting a Successful Incident Response*, 1–334. https://doi.org/10.1016/C2012-0-01092-7

Jovičić, B., & Simić, D. (2006). *Common Web Application Attack Types and Security Using ASP.NET*.

Kayes, A. S. M., Han, J., & Colman, A. (2014). OntCAAC: An Ontology-Based Approach to Context-Aware Access Control for Software Services. *Computer Journal*, *58*(11), 3000–3034. https://doi.org/10.1093/COMJNL/BXV034

Kayes, A. S. M., Rahayu, W., & Dillon, T. (2018). An ontology-based approach to dynamic contextual role for pervasive access control. *Proceedings - International Conference on Advanced Information Networking and Applications, AINA*, *2018-May*, 601–608. https://doi.org/10.1109/AINA.2018.00093

Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). *Survey of intrusion detection systems: techniques, datasets and challenges*. https://doi.org/10.1186/s42400-019-0038-7

Kügler, D. (2003). "Man in the middle" attacks on bluetooth. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *2742*, 149–161. https://doi.org/10.1007/978-3-540-45126-6_11/COVER

Liao, H. J., Richard Lin, C. H., Lin, Y. C., & Tung, K. Y. (2013). Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, *36*(1), 16–24. https://doi.org/10.1016/J.JNCA.2012.09.004

Lin, H. S., Spector, A. Z., Neumann, P. G., & Goodman, S. E. (2007). Toward a safer and more secure cyberspace. *Communications of the ACM*, *50*(10), 128. https://doi.org/10.1145/1290958.1290991

McIntosh, T., Jang-Jaccard, J., Watters, P., & Susnjak, T. (2019). The inadequacy of entropy-based ransomware detection. *Communications in Computer and Information Science*, *1143 CCIS*, 181–189. https://doi.org/10.1007/978-3-030-36802-9_20

Meng, W., Li, W., & Kwok, L. F. (2014). EFM: Enhancing the performance of signature-based network intrusion detection systems using enhanced filter mechanism. *Computers & Security*, *43*, 189–204. https://doi.org/10.1016/J.COSE.2014.02.006

Mohammadi, S., Mirvaziri, H., Ghazizadeh-Ahsaee, M., & Karimipour, H. (2019). Cyber intrusion detection by combined feature selection algorithm. *Journal of Information Security and Applications*, *44*, 80–88. https://doi.org/10.1016/J.JISA.2018.11.007

Ragsdale, D. J., Carver, C. A., Humphries, J. W., & Pooch, U. W. (2000). Adaptation techniques for intrusion detection and intrusion response systems. *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics*, *4*, 2344–2349. https://doi.org/10.1109/ICSMC.2000.884341

Reyhan Ghifari, R. (2023). *OJK: Akibat Kejahatan Siber, Dunia Rugi 8 T Dolar AS pada 2023*. https://tirto.id/ojk-akibat-kejahatan-siber-dunia-rugi-8-t-dolar-as-pada-2023-gSPd

Sarker, I. H. (2019). A machine learning based robust prediction model for real-life mobile phone data. *Internet of Things*, *5*, 180–193. https://doi.org/10.1016/J.IOT.2019.01.007

Sarker, I. H., Abushark, Y. B., & Khan, A. I. (2020). ContextPCA: Predicting context-aware smartphone apps usage based on machine learning techniques. *Symmetry*, *12*(4). https://doi.org/10.3390/SYM12040499

Sarker, I. H., & Salim, F. D. (2018). Mining user behavioral rules from smartphone data through association analysis. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *10937 LNAI*, 450–461. https://doi.org/10.1007/978-3-319-93034-3_36/COVER

Suaib Akhter, A. F. M., Ahmed, M., Shahen Shah, A. F. M., Anwar, A., Kayes, A. S. M., & Zengin, A. (2021). A blockchain-based authentication protocol for cooperative vehicular ad hoc network. *Sensors (Switzerland)*, *21*(4), 1–21. https://doi.org/10.3390/s21041273

Sun, N., Zhang, J., Rimba, P., Gao, S., Zhang, L. Y., & Xiang, Y. (2019). Data-Driven

ESCAF 3rd 2024
p-ISSN : 2962 - 7710
e-ISSN : 3021 - 8594

Cybersecurity Incident Prediction: A Survey. *IEEE Communications Surveys and Tutorials*, *21*(2), 1744–1772. https://doi.org/10.1109/COMST.2018.2885561

Tapiador, J. E., Orfila, A., Ribagorda, A., & Ramos, B. (2015). Key-Recovery Attacks on KIDS, a Keyed Anomaly Detection System. *IEEE Transactions on Dependable and Secure Computing*, *12*(3), 312–325. https://doi.org/10.1109/TDSC.2013.39

Tavallaee, M., Stakhanova, N., & Ghorbani, A. A. (2010). Toward credible evaluation of anomaly-based intrusion-detection methods. *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews*, *40*(5), 516–524. https://doi.org/10.1109/TSMCC.2010.2048428

Twomey, P. (2010). *Cyber Security Threats*.

Viegas, E., Santin, A. O., Franca, A., Jasinski, R., Pedroni, V. A., & Oliveira, L. S. (2017). Towards an Energy-Efficient Anomaly-Based Intrusion Detection Engine for Embedded Systems. *IEEE Transactions on Computers*, *66*(1), 163–177. https://doi.org/10.1109/TC.2016.2560839

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems*, *18*(2), 101–105. https://doi.org/10.1057/EJIS.2009.12/METRICS

Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., Gao, M., Hou, H., & Wang, C. (2018). Machine Learning and Deep Learning Methods for Cybersecurity. *IEEE Access*, *6*, 35365–35381. https://doi.org/10.1109/ACCESS.2018.2836950