Um Mapeamento Sistemático sobre Detecção de Ataques em Redes de Computadores

Gabrielly da Silva[1], **Carina Oliveira**[1], **Reinaldo Braga**[1]

[1]Laboratório de Redes de Computadores e Sistemas (LAR)
Instituto Federal de Educação, Ciência e Tecnologia do Ceará (IFCE)
Fortaleza – CE – Brazil

gabyrlsilva@gmail.com, {carina,reinaldo}@lar.ifce.edu.br

Abstract. *During the COVID-19 pandemic, there was a significant surge in news about companies being targeted by cybercriminals. In this context, research efforts aimed at reducing the impact of network attacks through Artificial Intelligence (IA) algorithms grown. Consequently, this research presents a systematic mapping in the context of detection of attack techniques on computer networks. Initially, this work identifying the most commonly employed algorithms and databases, as well as categorizing the types of attacks and the volume of samples. Subsequently, we address the absence of databases containing new attacks, sample imbalances, and solutions incorporating multiple AI algorithms.*

Resumo. *Durante a pandemia de COVID-19, houve uma grande repercussão de notícias sobre empresas sendo atacadas por cibercriminosos. Nesse contexto, cresceram as pesquisas que propunham diminuir o impacto dos ataques à rede com algoritmos de Inteligência Artificial (IA). Este trabalho apresenta um mapeamento sistemático no âmbito da detecção de ataques às redes de computadores. Inicialmente, são identificados os algoritmos e os bancos de dados mais utilizados, além disso, os tipos de ataques, assim como a quantidade de amostras. Posteriormente, expõe-se a ausência de bancos de dados com ataques atuais, o desequilíbrio de amostras e soluções de arquitetura com mais de um algoritmo de IA.*

1. Introdução

De acordo com o relatório da *Alliance Virtual Offices*, os ataques cibernéticos aumentaram em 238% durante a pandemia de COVID-19 [Report 2023]. Isso ocorreu por conta da mudança do trabalho presencial para o remoto, gerando um ambiente propício para ataques cibernéticos [Gatefy 2021]. Com o avanço tecnológico, software e hardware são atualizados constantemente e, com isso, o número de vulnerabilidades aumentam, assim como o nível de sofisticação de técnicas de ataques [Wang et al. 2012].

Normalmente, os softwares de monitoramento de rede geram alertas quando há um comportamento suspeito, tendo em seguida, um especialista encarregado de investigar se o alerta está relacionado a um ataque real (Verdadeiro Positivo) ou um alerta falso (Falso Positivo) [Brisse et al. 2021]. Os analistas de segurança têm como objetivos identificar, analisar e mitigar possíveis ataques na rede. Sendo que os alertas são analisados, na maioria das vezes, de forma manual, gerando uma fadiga de alertas [Ayala et al. 2021].

De acordo com a pesquisa desenvolvida pela *International Data Corporation* (IDC) para a *FireEye*, identificou-se que 45% dos alertas são falsos, gerando um trabalho interno menos eficiente e com baixo fluxo de solução de incidentes [Advisor 2021].

Para uma compreensão abrangente do campo de detecção de ataques, é importante identificar na pesquisa os algoritmos de Inteligência Artificial (IA) e os bancos de dados focados no tráfego de rede que são abordados na literatura. Portanto, para enriquecer o entendimento sobre esse tópico, é fundamental identificar e avaliar os estudos disponíveis.

Neste contexto, esse trabalho propõe um mapeamento sistemático sobre detecção de ataques, tendo como objetivos principais identificar os algoritmos utilizados e identificar os bancos de dados disponíveis, possibilitando a extração das características dos bancos encontrados, como quantidade de amostras e tipos de ataques.

Para alcançar tais objetivos, a metodologia proposta é dividida em três partes. A primeira consiste no planejamento da revisão da literatura, a segunda refere-se aos critérios determinados para filtrar os artigos e a terceira na construção de visualizações estratégicas. Levando em consideração a quantidade de artigos encontrados sobre detecção de ataques, o software *Rayyan* foi utilizado como ferramenta de análise de artigos. Os resultados obtidos servem para auxiliar estudantes, pesquisadores e/ou profissionais da área na tomada de decisão sobre o tipo de algoritmo e bancos de dados disponíveis para aplicar na detecção de ataques em redes de computadores.

2. Trabalhos Relacionados

Nesta seção são analisadas as soluções propostas na literatura sobre detecção de ataques. Para viabilizar o mapeamento sistemático, esta análise foi dividida em duas áreas de pesquisas: detecções com algoritmos IA e sistemas que recomendam mitigações para os ataques identificados.

2.1. Detecções com algoritmos de IA

Na literatura, algoritmos de IA são implementados para detectar os ataques, utilizando em seus experimentos bancos de dados públicos. Os autores de [Kilincer et al. 2021] realizaram um estudo com cinco *datasets*: CIC IDS 2018, UNSW-NB15, ISCX-2012, NSL-KDD, CIDDS-001, submetidos a três algoritmos: *Support Vector Machine* (SVM), *K-Nearest Neighbors* (KNN) e *Decision Tree* (DT). Com base nisso, compararam os resultados e o melhor resultado foi o DT.

Já os autores de [Abdallah et al. 2022] buscaram estudar o desempenho de classificadores com o conjunto de quatro *datasets*: KDD 99, NSL-KDD, CICIDS2017 e UNSW-NB15. Diferentes algoritmos como *Random Florest* (RF), SVM, *Artificial Neural Network* (ANN), *Quadratic Discriminant Analysis* (QDA) e *Deep Neural Network* (DNN) foram analisados e apontados com bons resultados em diferentes bases.

Esses trabalhos possuem uma revisão sobre diferentes algoritmos para bases públicas. Desta forma, observa-se que, por tratar-se de dados públicos, há um desequilíbrio dos dados, fazendo com que a seleção de atributos interfira no desempenho.

Portanto, quando algoritmos de IA são utilizados, é preciso entender como classificar o problema. Sendo assim, quando o atributo é binário, objetivando detectar o dado normal ou ataque, os algoritmos são eficazes, podendo-se identificar que a melhor

abordagem identificada no trabalho foi o DT [Dhanya et al. 2023]. No entanto, quando analisada a classificação com multi-classes, há vários algoritmos destacados, sendo difícil determinar o melhor algoritmo para a rede.

Vários ataques podem ser realizados ao mesmo tempo, sendo necessário classificar e priorizar esses ataques para estabelecer uma melhor defesa [Wang et al. 2012]. Na Figura 1 estão representados vários algoritmos encontrados nos trabalhos pesquisados usados neste trabalho. Os trabalhos [Kilincer et al. 2021] e [Dhanya et al. 2023] apresentam o detalhamento desses ataques.

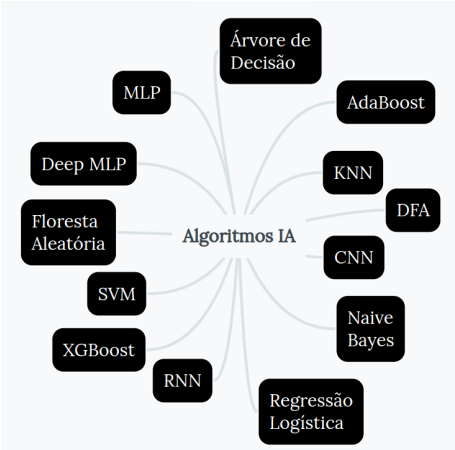

Figura 1. Resumo dos Algoritmos de IA citados.

2.2. Métodos de recomendação de mitigação

Para analisar as recomendações de mitigação, é importante apresentar interfaces para o usuário ou gráficos de ataques. Os autores de [Beran et al. 2020] criaram um banco de dados a partir de computadores afetados por incidentes, dividindo-o em um conjunto de demonstração da ferramenta e outro para avaliação. Por meio de métodos analíticos, foram analisados os *timestamps* para avaliar as alterações nos arquivos por meio da hora, o que resultou em um aplicativo, o *Filesystem Metadata Analysis* (FIMETIS).

De forma semelhante, o trabalho de [Ayala et al. 2021] tem como objetivo apresentar uma interface de usuário para recomendar mitigações de ataques, utilizando *datasets* públicos como OWASP, NIST e CSIRT. A interação de um analista com a ferramenta visual proposta nos trabalhos auxilia na minimização do tempo de resposta a um ataque. Porém, as validações foram realizadas com poucos especialistas e os estudos não utilizaram uma ampla variedade de ataques.

3. Metodologia

Tendo como objetivo identificar, avaliar e interpretar as pesquisas disponíveis, a metodologia adotada para este mapeamento sistemático foi baseada no guia do trabalho de [Kitchenham and Charters 2007], que está dividido em três fases: planejamento, condução e resultado.

3.1. Planejamento

Nessa etapa, procura-se gerar um critério de busca para padronizar a pesquisa de artigos em repositórios como *Wiley, Scielo, IEEExplore, ACM Digital Library, ScienceDirect* e

SpringerLink. Com o auxílio da Tabela 1, que apresenta a tabela População, Intervenção, Comparação e *Outcomes* (PICO), busca-se compreender melhor sobre as redes que apresentam maior vulnerabilidade de serem atacadas por *cyber attacks*. Também por meio da Tabela 1, padronizou-se as *strings* de busca que auxiliam na pesquisa dos repositórios. Para avaliar os artigos encontrados, os critérios de inclusão e exclusão foram gerados para filtrar os artigos encontrados.

Tabela 1. Tabela PICO adaptada [da Costa Santos et al. 2007].

Elemento	Descrição	Palavras-chaves
População	Todas as redes que são foco dos cibercriminosos	*Cyber Attack*
Intervenção	Detecção dos alertas falsos positivos e detecção das técnicas/táticas na rede	*Intrusion Detection, Anomaly, Signature*
Comparação	Comparar soluções de IA e *datasets* utilizados	*Deep Learning, Machine Learning*
Resultados	Verificar a efetividade dos resultados obtidos	-

Os critérios de inclusão foram: artigos que abordam algoritmos de IA para detecção de ataques; que identificam o tipo de banco de dados usado; artigos escritos em inglês e português; que possuem uma acurácia maior que 70%.

Os critérios de exclusão foram: trabalhos duplicados (com o auxílio do software *Rayyan*, foram feitas varreduras de duplicidade); trabalhos fora do contexto; trabalho que apresentam bancos de dados sem possibilidade de análise; e trabalhos que apresentam experimentos sem análise comparativa. Conforme mostra a Figura 2, houve um crescimento rápido em pesquisas relacionadas à detecção de ataques a partir de 2017, havendo um ápice no período da pandemia, por conta do aumento dos ataques cibernéticos. Assim, esse trabalho também utilizou como critério de exclusão os artigos escritos antes de 2017.

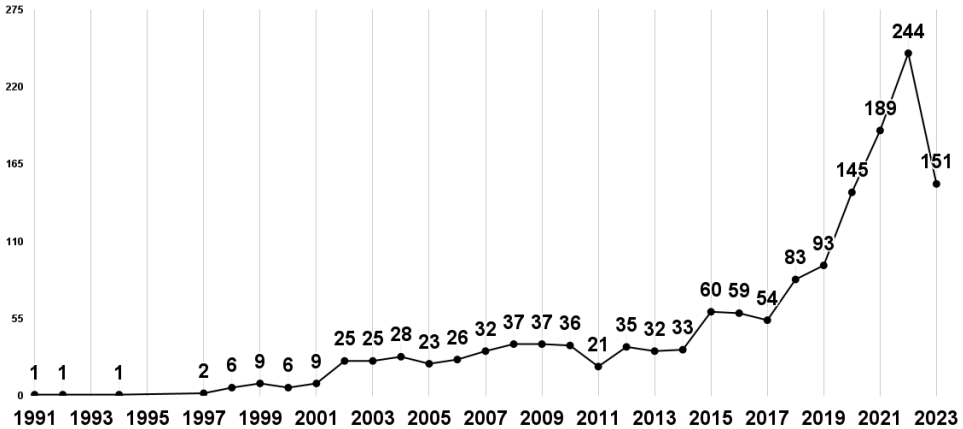

Figura 2. Quantidade de pesquisas por ano.

3.2. Condução

Seguindo o planejamento, usando as palavras-chaves da Tabela 1 nos repositórios, obteve-se cerca de 5.346 artigos. Sendo que, em cada repositório eram selecionados no máximo 1000 artigos. Com a filtragem de duplicidade e fora do contexto de detecção de ataques, chegou-se 1.507 artigos. Com base nisso, aplicando o critério de exclusão com o corte

do ano de 2017, chegou-se a 534 artigos. Como não é viável analisar criticamente mais de 500 artigos, buscou-se extrair artigos que apresentavam algoritmos IA e bancos de dados disponíveis para *download*. Com isso, foram selecionados 23 artigos, sendo 17 publicados em *journals* e 6 em conferências.

4. Resultados

Nesta seção, destaca-se os 23 artigos mostrados na Tabela 2 para determinar os algoritmos citados e identificar os tipos de bancos de dados, assim como a quantidade de amostras e tipos de ataques.

Tabela 2. Trabalhos selecionados.

ID	Referência	ID	Referência	ID	Referência
1	[Kilincer et al. 2021]	9	[Mushtaq et al. 2022]	17	[Sayed et al. 2022]
2	[Dhanya et al. 2023]	10	[Gaber et al. 2022]	18	[Cerda et al. 2021]
3	[Kim et al. 2017]	11	[Patgiri et al. 2018]	19	[Bentes et al. 2021]
4	[Siddiqi and Pak 2022]	12	[Attou et al. 2023]	20	[Almseidin et al. 2017]
5	[Wu et al. 2022]	13	[Karthika and Maheswari 2022]	21	[Lucas et al. 2021]
6	[Jain et al. 2022]	14	[Hnamte and Hussain 2023]	22	[Kanimozhi and Jacob 2021]
7	[Sousa and Silva 2022]	15	[Vishwakarma and Kesswani 2023]	23	[Leevy et al. 2021]
8	[Sarhan et al. 2022]	16	[Aminanto et al. 2022]		

4.1. Algoritmos de IA

Na detecção de ataques, é importante identificar os algoritmos presentes na literatura. Com isso, gerou-se a Figura 3, em que são apresentados os algoritmos citados pelos autores dos artigos presentes na Tabela 2, com o intuito de analisar quais algoritmos são mais citados dentro da literatura.

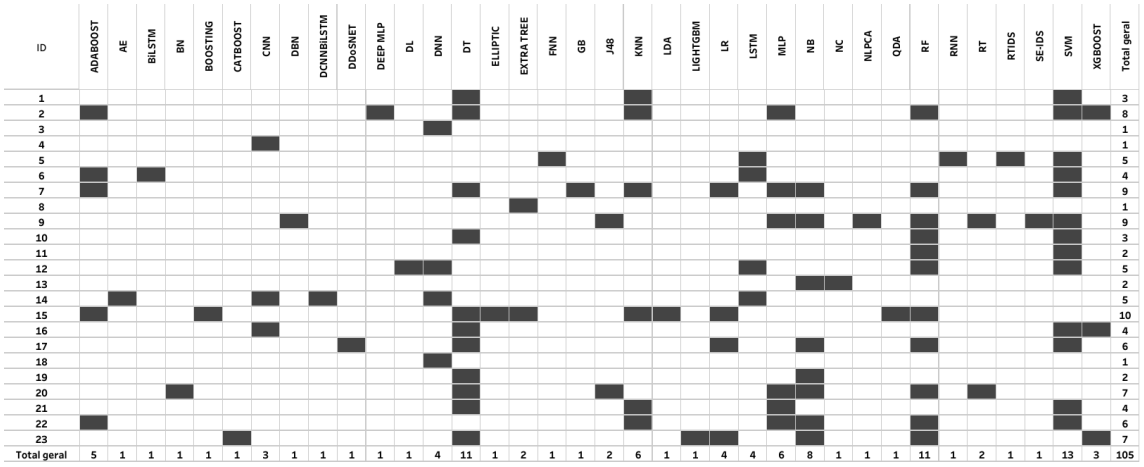

Figura 3. Visão geral entre autores e algoritmos.

No total, foram identificados 36 algoritmos de implementação para detectar ataques. De imediato, pode-se destacar o *Support Vector Machine* (SVM), o *Decision Tree* (DT) e *Random Forest* (RF) como os principais algoritmos utilizados nessa área. Além disso, dentre os 23 artigos, ambos os algoritmos foram citados 13, 11 e 11 vezes, respectivamente, o que indica que são algoritmos de comparação nas pesquisas.

Também deve-se levar em consideração o total de algoritmos estudada por cada trabalho, conforme mostra a última coluna da Figura 3. Há trabalhos em que a comparação faz parte da proposta para compreender o motivo das decisões tomadas, em contrapartida, o uso de apenas um algoritmo para análise não deve ser descartado, sendo que a mudança de parâmetros pode ser um método comparativo. O trabalho com maior número de algoritmo foi o de ID 15 [Vishwakarma and Kesswani 2023], com 10 algoritmos.

4.2. Bancos de dados

Na Figura 4, pode-se obter uma visão geral da quantidade de vezes em que cada banco de dados foi utilizado nos trabalhos selecionados, com isso, observou-se 15 bancos presentes. Tendo em vista esses dados, observa-se que há uma frequência no uso dos bancos: CIC IDS 2018, UNSW-NB15, NSL-KDD e CIC IDS 2017.

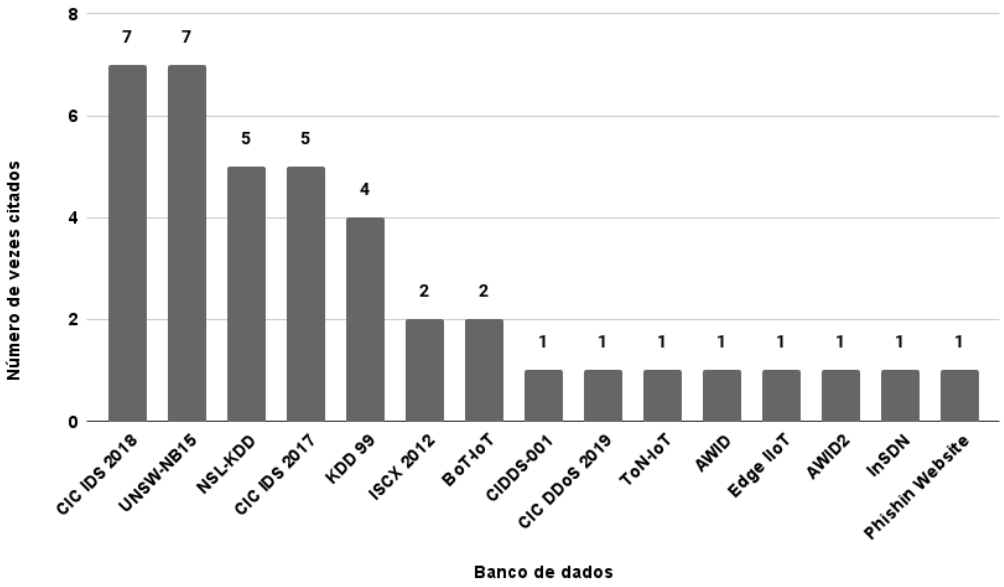

Figura 4. Visão geral entre banco de dados e número de citações.

Acredita-se que esses bancos são os mais citados por apresentarem uma diversidade de ataques como pode-se ver na Tabela 3. Além disso, observando-se as porcentagens que cada ataque representa no banco, fica perceptível o desequilíbro dos dados, fazendo-se necessário um pré-processamento, o que pode variar de acordo com a escolha de cada autor. Logo, esse desequilíbrio dificulta a detecção de cada tipo de ataque usando aprendizagem de máquina.

Dentre todos os bancos analisados, o ISCX 2012 não está presente na Tabela 3 porque apresentou arquivos maiores que 10G, dificultando a análise. De forma geral, quando observados os ataques, é possível visualizar que os ataques de *Denial of Service* (DoS) e *Distributed Denial of Service* (DDoS) estão presentes na maioria dos bancos de dados. Isso pode facilitar uma correlação entre bancos por meio de ataques.

Em contrapartida, os outros ataques são diferentes, o que faz com que nenhum desses bancos de dados abranja todos os ataques de forma completa. Isso também implica

Tabela 3. Ataques presentes nos bancos de dados e a representação percentual dentro da amostra total.

Banco de dados	Ataques (%)	Total de Amostras
CIC IDS 2018	Benign (86%), Brute Force (2%), DoS (3,2%), DDoS (6,2%), Injection (0,0004%), Infilteration (0,8%), Botnet (1,4%)	20.253.943
UNSW-NB15	Benign (87%), Exploits (1,7%), DoS (0,64%), ShellCode (0,07%), Reconnaissance (0,55%), Fuzzers (0,95%), Generic (8,5%), Analysis (0,11%), Backdoors (0,09%), Worms (0,01%)	2.540.218
NSL-KDD	Benign (51,8%), DoS (36%), Probe (9,5%), Privilege Escalation (0,13%), Remote Access (2,6%)	148.597
CIC IDS 2017	Benign (79,5%), DDoS (4,7%), PortScan (5,8%), Botnet (0,07%), Infiltration (0,0013%), BruteForce (0,06%), XSS (0,02%), Injection (0,0008%), Patator (0,5%), DoS (9,3%), Heartbleed (0,0004%)	2.715.743
KDD 99	Benign (19,7%), DoS (79%), Probe (0,83%), Privilege Escalation (0,011%), Remote Access (0,23%)	494.020
BoT-IoT	Benign (0,013%), Reconnaissance (2,5%), DoS (44,3%), Theft (0,002%), DDoS (53,2%)	72.470.463
CIDDS-001	Benign (88,2%), Suspicious (1,4%), Unknown (0,24%), Attacker (5,2%), Victim (5%)	31.959.174
CIC DDoS 2019	Bening (0,2%), PortMap (0,4%), NetBIOS (5,4%), LDAP (4%), MSSQL (11,7%), UDP (8,6%), SYN (13,1%), DrDoS (56,7%), DDoS (0,001%), TFTP (-)	49.319.810
ToN-IoT	Benign (28,5%), Backdoor (2,4%), Password (5,2%), DDoS (20,4%), Injection (2%), Ransomware (0,28%), XSS (6,8%), Scanning (20%), DoS (14,6%), MITM (0,004%)	31.502.397
AWID	Benign (91,2%), Impersonation (2,9%), Injection (3,4%), Flooding (2,4%)	1.795.575
EDGE IIoT	Benign (53,5%), Backdoor (0,12%), DDoS (40%), MITM (0,006%), Fingerprinting (0,005%), Password (5%), Port Scanning (0,11%), Ransomware (0,05%), Injection (0,24%), Uploading (0,18%), Vulnerability Scanner (0,7%), XSS (0,08%)	20.939.622
AWID 2	Benign (89%), Impersonation (3,6%), Injection (4,3%), Flooding (3%)	1.893.518
InSDN	Benign (20%), DDoS (35,5%), Probe (28,5%), DoS (15,6%), BFA (0,41%), U2R (0,005%), Web Attack (0,06%), Botnet (0,05%)	343.889
PHISHING	Benign (55,7%), Phishing (44,3%)	11.055

no ano em que os bancos foram criados, como visto anteriormente, a tecnologia está em evolução a cada instante, o que faz com que os ataques sejam melhorados e mais difíceis de serem detectados.

5. Conclusão

O principal objetivo deste trabalho foi mapear sistematicamente as detecções de ataques identificando os algoritmos de IA e os bancos de dados abordados na literatura. Como observado, com o decorrer dos anos, a detecção de ataque ainda é bastante explorada, mostrando assim, que mesmo apresentando métodos para solucionar o problema, ainda não foi resolvido.

Em relação aos algoritmos, principalmente SVM, *Decision Tree* e *Random Forest*, apresentam maior influência para detectar ataques, levando em consideração a quantidade de citações que propõe o uso desses algoritmos. Uma alternativa futura, é criar uma arquitetura em que mais de um algoritmo seja implementado, aproveitando as melhores características das técnicas propostas.

Infere-se também que os bancos de dados, CIC IDS 2018, UNSW-NB15 e NSL-KDD são os principais dentro da literatura. Apresentam variedades de ataques e analisam os dados de tráfego de rede. No entanto, os dados foram capturados antes de 2019, mesmo

que esse trabalho esteja estudando trabalhos entre 2017 a 2023, os bancos de dados apresentados não representam os ataques atuais com técnicas sofisticadas. Mostra-se então que a criação de um *dataset* com informações de ataques recentes é uma possibilidade de estudo futuro.

Por meio desse trabalho, conseguiu-se identificar a ausência de banco de dados com os novos ataques que surgem no decorrer dos anos, o grande desequilíbrio que há das amostras e uma arquitetura que engloba mais de um algoritmo para detectar ataques. Além disso, há possibilidade de criar parâmetros para cada tipo de ataque e exibir a gravidade do ataque, além de apenas determinar se é um dado normal ou ataque, o que auxilia na mitigação de ataques.

Referências

Abdallah, E. E., Eleisah, W., and Otoom, A. F. (2022). Intrusion detection systems using supervised machine learning techniques: A survey. *Procedia Computer Science*, 201:205–212.

Advisor, C. (2021). Alerta causa fadiga e queda de produtividade de equipes no soc.

Almseidin, M., Alzubi, M., Kovacs, S., and Alkasassbeh, M. (2017). Evaluation of machine learning algorithms for intrusion detection system. In *2017 IEEE 15th International Symposium on Intelligent Systems and Informatics (SISY)*, pages 000277–000282.

Aminanto, M. E., Wicaksono, R. S. H., Aminanto, A. E., Tanuwidjaja, H. C., Yola, L., and Kim, K. (2022). Multi-class intrusion detection using two-channel color mapping in ieee 802.11 wireless network. *IEEE Access*, 10:36791–36801.

Attou, H., Guezzaz, A., Benkirane, S., Azrour, M., and Farhaoui, Y. (2023). Cloud-based intrusion detection approach using machine learning techniques. *Big Data Mining and Analytics*, 6(3):311–320.

Ayala, C., Jimenez, K., Loza-Aguirre, E., and Andrade, R. O. (2021). A hybrid recommender system for cybersecurity based on a rating approach. In Daimi, K., Arabnia, H. R., Deligiannidis, L., Hwang, M.-S., and Tinetti, F. G., editors, *Advances in Security, Networks, and Internet of Things*, pages 397–409, Cham. Springer International Publishing.

Bentes, E., Figueiredo, Y., and Campos, L. (2021). Aplicação de algoritmos de aprendizado de máquina para detecção de intrusão. In *Anais Estendidos do XXXIX Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, pages 209–216, Porto Alegre, RS, Brasil. SBC.

Beran, M., Hrdina, F., Kouřil, D., Ošlejšek, R., and Zákopčanová, K. (2020). Exploratory analysis of file system metadata for rapid investigation of security incidents. In *2020 IEEE Symposium on Visualization for Cyber Security (VizSec)*, pages 11–20, Salt Lake City, UT, USA,. Institute of Electrical and Electronics Engineers Inc.

Brisse, R., Boche, S., Majorczyk, F., Lalande, J.-F., and Lalande, J.-F. (2021). Kraken: A knowledge-based recommender system for analysts, to kick exploration up a notch. Technical report.

Cerda, B. M., Yuan, S., and Chen, L. (2021). Phishing detection using deep learning. In Daimi, K., Arabnia, H. R., Deligiannidis, L., Hwang, M.-S., and Tinetti, F. G.,

editors, *Advances in Security, Networks, and Internet of Things*, pages 117–128, Cham. Springer International Publishing.

da Costa Santos, C. M., de Mattos Pimenta, C. A., and Nobre, M. R. C. (2007). The pico strategy for the research question construction and evidence search. *Revista Latino-Americana de Enfermagem*, 15:508–511.

Dhanya, K., Vajipayajula, S., Srinivasan, K., Tibrewal, A., Kumar, T. S., and Kumar, T. G. (2023). Detection of network attacks using machine learning and deep learning models. *Procedia Computer Science*, 218:57–66.

Gaber, T., El-Ghamry, A., and Hassanien, A. E. (2022). Injection attack detection using machine learning for smart iot applications. *Physical Communication*, 52:101685.

Gatefy (2021). Como o covid-19 impactou os crimes cibernéticos, segundo a europol. Acesso em: 05 mar. 2023.

Hnamte, V. and Hussain, J. (2023). Dcnnbilstm: An efficient hybrid deep learning-based intrusion detection system. *Telematics and Informatics Reports*, 10:100053.

Jain, S., Pawar, P. M., and Muthalagu, R. (2022). Hybrid intelligent intrusion detection system for internet of things. *Telematics and Informatics Reports*, 8:100030.

Kanimozhi, V. and Jacob, T. P. (2021). Artificial intelligence outflanks all other machine learning classifiers in network intrusion detection system on the realistic cyber dataset cse-cic-ids2018 using cloud computing. *ICT Express*, 7(3):366–370.

Karthika, R. and Maheswari, M. (2022). Detection analysis of malicious cyber attacks using machine learning algorithms. *Materials Today: Proceedings*, 68:26–34. 6th International Conference on Recent Advances in Material Chemistry.

Kilincer, I. F., Ertam, F., and Sengur, A. (2021). Machine learning methods for cyber security intrusion detection: Datasets and comparative study. *Computer Networks*, 188:107840.

Kim, J., Shin, N., Jo, S. Y., and Kim, S. H. (2017). Method of intrusion detection using deep neural network. In *2017 IEEE International Conference on Big Data and Smart Computing (BigComp)*, pages 313–316, Jeju. IEEE.

Kitchenham, B. A. and Charters, S. (2007). Guidelines for performing systematic literature reviews in software engineering (ebse 2007-001). Technical report, Keele University and Durham University Joint Report.

Leevy, J. L., Hancock, J., Zuech, R., and Khoshgoftaar, T. M. (2021). Detecting cybersecurity attacks across different network features and learners. *Journal of Big Data*, 8(1):38.

Lucas, T., Costa, K., Moraes, E., Júnior, P. H., and Neves, M. (2021). Stacking-based committees para detecção de ataques em redes de computadores - uma abordagem por exaustão. In *Anais do XXXIX Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, pages 644–657, Porto Alegre, RS, Brasil. SBC.

Mushtaq, E., Zameer, A., and Khan, A. (2022). A two-stage stacked ensemble intrusion detection system using five base classifiers and mlp with optimal feature selection. *Microprocessors and Microsystems*, 94:104660.

Patgiri, R., Varshney, U., Akutota, T., and Kunde, R. (2018). An investigation on intrusion detection system using machine learning. In *2018 IEEE Symposium Series on Computational Intelligence (SSCI)*, pages 1684–1691.

Report, S. (2023). Ataques cibernéticos no trabalho remoto mais que triplicaram durante a pandemia.

Sarhan, M., Layeghy, S., Moustafa, N., and Portmann, M. (2022). Towards a standard feature set of nids datasets. *Mobile Networks and Applications*.

Sayed, M. S. E., Le-Khac, N.-A., Azer, M. A., and Jurcut, A. D. (2022). A flow-based anomaly detection approach with feature selection method against ddos attacks in sdns. *IEEE Transactions on Cognitive Communications and Networking*, 8(4):1862–1880.

Siddiqi, M. A. and Pak, W. (2022). Tier-based optimization for synthesized network intrusion detection system. *IEEE Access*, 10:108530–108544.

Sousa, W. T. M. and Silva, C. A. (2022). Análise de desempenho em algoritmos de aprendizagem de máquina na detecção de intrusão baseada em fluxo de rede usando o conjunto de dados unsw-nb15. *Revista de Sistemas e Computação*, 12(2):51–57.

Vishwakarma, M. and Kesswani, N. (2023). A new two-phase intrusion detection system with naïve bayes machine learning for data classification and elliptic envelop method for anomaly detection. *Decision Analytics Journal*, 7:100233.

Wang, J. A., Guo, M., Wang, H., and Zhou, L. (2012). Measuring and ranking attacks based on vulnerability analysis. *Information Systems and e-Business Management*, 10(4):455–490.

Wu, Z., Zhang, H., Wang, P., and Sun, Z. (2022). Rtids: A robust transformer-based approach for intrusion detection system. *IEEE Access*, 10:64375–64387.