Cost-Based Analysis of Signature-Based NIDS and Anomaly-Based NIDS

Justin Wasser

University of Maryland Global Campus

ITEC 630: Intrusion Detection and Intrusion Prevention

Professor Choi

6/16/2023

Contents

Abstract

Signature-based network IDSes and anomaly-based network IDSes differ in their methodology for detecting intrusions into the networks they safeguard. This leads to each system having different relative strengths and weaknesses regarding reliability and computing resource consumption. To that point, both approaches to network intrusion detection will be assessed in terms of their detection accuracy and the amount of resources they require to operate. Moreover, the relative cost of NIDS inaccuracy will be explored. Lastly, a determination will be reached about the types of network environments where signature-based detection would be the most cost-effective detection methodology for a NIDS deployment.

Introduction

The ensuing research paper examines the intersection of detection accuracy and deployment cost regarding network intrusion detection systems (NIDS). More specifically, how the relatively less costly signature-based NIDS is likely to be the most cost-effective NIDS deployment option for organizations that have low occurrences of attempted network intrusions and a limited amount of resources to spend on network security.

To explore this topic NIDS will be discussed in terms of the two major approaches to intrusion detection, i.e., signature-based and anomaly-based (Scarfone & Mell, 2012). However, first, a cursory overview of intrusion detection systems will be required. Next, an in-depth analysis will be conducted on each detection methodology with a specific focus on the difference in the amount of computing resources required to implement each NIDS architecture. Furthermore, this will lead to a more comprehensive analysis of the relative strengths and weaknesses of each detection methodology. Finally, a conclusion will be reached as to which detection methodology would be best to utilize for enterprises with low occurrences of attempted network intrusions where keeping costs low is a major priority.

Intrusion Detection System (IDS) Overview

Intrusion detection refers to “the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents” (Scarfone & Mell, 2012). Furthermore, “an intrusion detection system (IDS) is software that automates the intrusion detection process” (Scarfone & Mell, 2012). What constitutes an ‘incident’ varies based both based on the detection method employed (signature-based or anomaly-based) and the detection specifications input into the system (Scarfone & Mell, 2012). Additionally, unlike an “intrusion prevention system (IPS)” (Scarfone & Mell, 2012) which can act on its own, an IDS merely creates an alert to warn a human of a possible incident (Scarfone & Mell, 2012). Ultimately, with an IDS it is up to the human reviewing the alerts whether to act or not (Scarfone & Mell, 2012).

The fundamental purpose of an Intrusion Detection System (IDS) is the same as any other network/system security technology, which is to protect the information stored within the network from threats that would compromise the information’s reliability, value, or ability to be leveraged by the owner of the network (Fortinet, n.d.). The accepted term for this aim in the field of network security is the “CIA Triad” (Fortinet, n.d.) with the CIA standing for “Confidentiality, Integrity, and Availability” (Fortinet, n.d.). Moreover, the most effective way to preserve networks/systems and the information contained within them from attacks that threaten their CIA is by building a security architecture that is layered so that there is no single point of failure within a security deployment (Fortinet, n.d*; Session 1: Introduction and Course Overview*, 2022). To that point, the layer of security that “network-based intrusion detection systems (NIDS)” (*Session 1: Introduction and Course Overview*, 2022) provides is to the network layer (*The OSI Reference Model Explained*, n.d.) Lastly, to appreciate the capabilities and limitations of different types of network-based IDSes (NIDS) we must first understand their architectures.

Signature-Based and Anomaly-Based NIDS Architectures

Network-based IDSes’ data collection and management architecture is comprised of four major components, “sensors” (Scarfone & Mell, 2012), a “management server” (Scarfone & Mell, 2012), a “database server” (Scarfone & Mell, 2012), and lastly a “console” (Scarfone & Mell, 2012). The NIDS architecture begins with sensors, as they are responsible for the collection of network traffic data (Scarfone & Mell, 2012). Furthermore, the quantity and specific placement of NIDS sensors depend upon the size and architecture of the network environment where the NIDS is being deployed (Scarfone & Mell, 2012). Moreover, sensors can be deployed in one of two ways, either they can be deployed "inline" (Scarfone & Mell, 2012) where network traffic must pass through the sensor or they can be deployed passively, where a copy of the network traffic is relayed to the NIDS interface (Scarfone & Mell, 2012). Each deployment architecture has its costs and benefits, but generally, passive sensors should be used for IDSes as the main benefit of inline sensors is they can take preventative measures when detection rules are matched, which is not a feature of IDSes (only IPSes) (Scarfone & Mell, 2012; Stallings, 2007). Furthermore, the NIDS management server "is a centralized device" (Scarfone & Mell, 2012) that collects all the network data provided by the sensors and analyzes it according to its specific detection rules (Scarfone & Mell, 2012). Next, all historical network events are stored in a database server so they can be accessed as needed (Scarfone & Mell, 2012). Lastly, a console is a software application that provides an interface for the user/administrator to examine the data provided by the NIDS and adjust the NIDS' configuration (Scarfone & Mell, 2012).

While the preceding paragraph described the general data collection and management architecture of NIDS the ensuing section will examine the processes that the two different detection approaches (signature-based and anomaly-based) must undergo to effectively analyze data that was collected from a network (Otoum & Nayak, 2021).

Signature-Based NIDS Methodology

As just mentioned, signature-based and anomaly-based detection are the two distinct approaches that network intrusion detection systems can utilize to identify threats (Otoum &

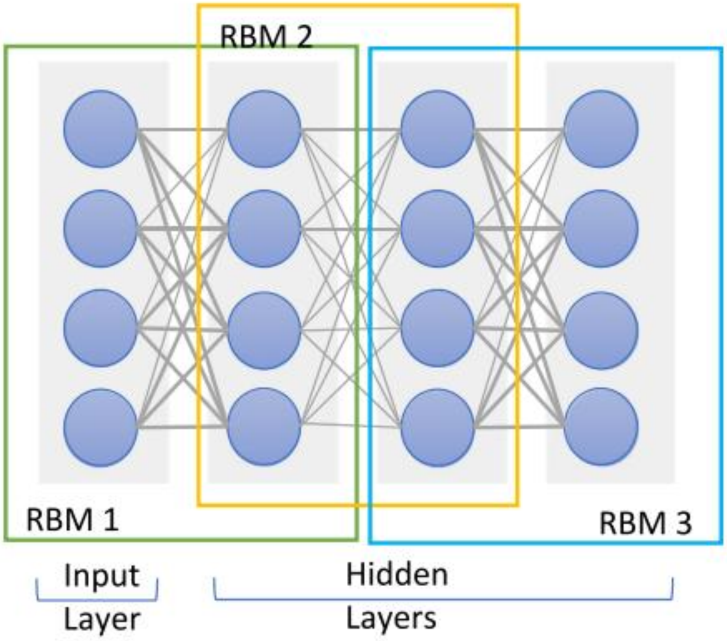
Nayak, 2021). Furthermore, both approaches consist of three-part processes that accomplish similar goals at each step but differ in specifics due to the requirements of each approach (Joshi & Hadi, 2015; Sourcefire, n.d.). For signature-based NIDS to function optimally, a three-part process consisting of packet decoding, packet preprocessing, and packet analysis (signature detection), must be followed in order (Sourcefire, n.d.). To that point, first, the "packet decoder" (Sourcefire, n.d.) takes an amount of raw network traffic data and makes it easier to analyze by adding "pointers to critical data locations" (Sourcefire, n.d.). These indicators are placed within the raw data to separate the ethernet, internet protocol (IP), and transmission control protocol (TCP) headers from each other and the data payload (Sourcefire, n.d.). Next, data is run through preprocessors, the goals of which are to further standardize data to make it easier to analyze, to "provide detection for attacks and activity not able to be done by standard snort rules" (Sourcefire, n.d.) and to reassemble data so messages are viewed in the correct order (Sourcefire, n.d.). Moreover, any number of unique preprocessors may be utilized by a signature-based NIDS and they execute "in the order they are loaded" (Sourcefire, n.d.). After being run through preprocessors, packets are analyzed via the NIDS' "detection engine" (Sourcefire, n.d.) which is looking to see if any patterns in the network traffic data match any known signatures of malicious activity (Scarfone & Mell, 2012; Sourcefire, n.d.). At this point a brief overview of how anomaly-based NIDS functions is required.

Anomaly-Based NIDS Methodology

For starters, anomaly-based detection is by its very nature more complex than signature-based detection as many network occurrences can be deemed anomalous (compared to the established network baseline) while a signature either matches or it does not (Scarfone & Mell, 2012). With that said, for anomaly-based NIDS to function optimally, a three-part process consisting of data set selection, preprocessing, and data analysis, must be conducted (Joshi & Hadi, 2015). First, to compare various anomaly-based IDSes against one another in terms of their accuracy, the same data set must be used for each anomaly-based IDS (Davis & Clark, 2011; Joshi & Hadi, 2015). Many datasets have been used for this purpose including the most widely used "KDD Cup 99 dataset" (Davis & Clark, 2011). Moreover, each data set contains two sections, first is the training portion of the data set used to train the chosen data mining algorithm, and the second is the testing portion of the data set used to evaluate the accuracy of the IDS (Khraisat et al., 2019). Next, after a particular data set has been selected it must undergo preprocessing (Khraisat et al., 2019).

Preprocessing refers to smoothing a given data set by removing any "incomplete or inconsistent" (Joshi & Hadi, 2015) information to facilitate more consistent analysis (Joshi & Hadi, 2015; Khraisat et al., 2019). To that point, there are several methods of preprocessing, including data "normalization" (Larriva-Novo et al., 2021) and "standardization" (Larriva-Novo et al., 2021) both of which increase the uniformity of the data set while reducing its size; while "feature selection" (Khraisat et al., 2019) and "discretization" (Joshi & Hadi, 2015) also accomplish similar goals. To that point, feature selection has two techniques which are "wrapper and filter methods" (Khraisat et al., 2019). The wrapper feature select method is used to reduce the size of the data being analyzed by estimating "subgroups of variables to identify the feasible interactions between variables" (Khraisat et al., 2019) as opposed to analyzing the entire variable (Khraisat et al., 2019). Moreover, the filter feature select method is used to rank features outside of any machine learning algorithm according to "their scores in several statistical tests for their correlation with the consequence variable" (Khraisat et al., 2019). Similarly, discretization-based preprocessing also involves manipulating variables, however, in these instances the goal is to transform infinite variables into discrete variables (Joshi & Hadi, 2015). Furthermore, there are four methods for discretization-based preprocessing and they all involve creating a "cut-point" (Joshi & Hadi, 2015) in the infinite variable which thereby transforms it into a discrete value (Joshi & Hadi, 2015). Ultimately, a more consistent data set is produced by preprocessing, which is beneficial during the next stage of the anomaly-based detection process, i.e., data mining (Joshi & Hadi, 2015).

For starters, data mining is a computing resource-intensive process that is essential to anomaly-based intrusion detection systems and this area has been the main focus of novel anomaly-based NIDS methodologies (Comito & Talia, 2017). Traditional data mining techniques, including machine learning (ML), could learn after being sufficiently trained on a data set, however, ML generally requires supervised input from humans to preprocess data for ML algorithms to learn from a given data set (Gyamfi & Jurcut, 2022; IBM Data and AI Team, 2023). However, newer data mining techniques often use some variation of Deep Learning (DL) because of its ability to train itself, i.e., "unsupervised learning" (Aldweesh et al., 2019), with no prior preprocessing of data by humans (Aldweesh et al., 2019). The underlying architecture of DL is exponentially more complex than ML as DL functions by "learning to represent the world as nested hierarchy of concepts, with each concept defined in relation to simpler concepts, and more abstract representations computed in terms of less abstract ones" (Aldweesh et al., 2019). The result is a vast web of sub-algorithms learning and refining knowledge from one another to create new knowledge as represented by the following illustration (Aldweesh et al., 2019).



(Aldweesh et al., 2019)

Regardless of the approach (signature or anomaly), the ultimate goal of any NIDS is to produce the most accurate assessments of network activity, that is, the ability to differentiate normal network traffic from malicious traffic (Gyamfi & Jurcut, 2022). To that point, a NIDS' ability can be measured by several criteria, however for the purposes of this paper the focus will be based on their propensity for "false positives" (Joshi & Hadi, 2015) otherwise known as "false alarms" (Gyamfi & Jurcut, 2022). Moreover, this assessment criteria is supported by Gyamfi & Jurcut (2022) who state that "the performance of an NIDS can be determined based on the Detection Rate (DR) and the False Alarm Rate (FAR)" (Gyamfi & Jurcut, 2022). Therefore, while the false positive/false alarm rate is not the only measurement of a NIDS' accuracy, it is a vital component of it (Gyamfi & Jurcut, 2022; Joshi & Hadi, 2015)

Comparing and Contrasting Signature-Based NIDS and Anomaly-Based NIDS

For starters, the relative simplicity of signature-based NIDS compared to anomaly-based NIDS makes its implementation and deployment much less costly (*What Are the Pros and Cons of Signature-Based vs. Anomaly-Based Detection?*, n.d.). Further adding to this cost discrepancy is the fact that signature-based NIDS does not need to be trained (and continuously re-trained) to function (Scarfone & Mell, 2012). Additionally, this architecture allows organizations the flexibility to "subscribe to signature packages released by expert developers" (*Session 2: Network-Based Intrusion Detection*, 2022), thereby saving considerable costs associated with employing/contracting expert network security personnel (*Session 11: Output Plug-Ins and Operational Use*, n.d.). Furthermore, an additional benefit of signature-based NIDS is increased accuracy compared to anomaly-based detection, as signature-based NIDSes are "more reliable (less false negatives), provide less false positives, and allow for easier false positive resolution" (S et al., 2020). However, the main drawback of signature-based NIDS is its inability to detect novel attacks (zero-day attacks) (Scarfone & Mell, 2012).

The ability to detect novel attacks is the largest differentiator between the two intrusion detection approaches as that is signature-based detection's greatest weakness, while it is anomaly-based detection's greatest strength (Scarfone & Mell, 2012). However, anomaly-based NIDS is not without its weaknesses. For starters, because anomaly-based NIDS requires a uniform data set to compare results between different anomaly detection models/algorithms, there is potential for the data sets being used to become outdated (Aldweesh et al., 2019). This appears to have occurred with popular datasets as a study reviewing anomaly-based IDSes found that "current proposed deep learning-based IDS do not provide reliable performance results, since they rely on the KDD99 or NSL-KDD benchmark datasets, which contain old traffic, do not represent recent attack scenarios and traffic behaviours [sic], and do not have real-time properties” (Aldweesh et al., 2019). Moreover, another similar literature review found this was a widespread issue as they found that “60% of the proposed methodologies were tested using KDD Cup'99 and NSL-KDD datasets” (Ahmad et al., 2020).

Furthermore, another weakness of anomaly-based NIDS is the cost associated with training anomaly-based models, especially considering according to a study conducted by Ahmad et al. (2020), 80% of novel anomaly-based NIDS utilize Deep Learning (DL) as part of their detection methodologies (Ahmad et al., 2020). As explained earlier, the benefit of DL is their ability to learn without human assistance via preprocessing data, however, the cost of this advancement is DL-based anomaly NIDSes “require high resources in terms of computational power, storage capacity, and time” (Ahmad et al., 2020). Moreover, this resource cost begins with training the model as “with deep learning, cross-validation increases training cost” (Aldweesh et al., 2019) and continues throughout its deployment as “In a network, models should be retrained frequently” (Abbasi et al., 2021). Lastly, this cost will only continue to rise as DL-based anomaly NIDSes become more advanced because “When the deep network goes deeper with a large number of layers and neurons, the computation complexity increases” (Aldweesh et al., 2019). This is affirmed by a study by Comito & Talia (2017) which shows a strong positive correlation between the “number of instances” (Comito & Talia, 2017), i.e., a measurement of data, and the amount of energy and time required by data mining algorithms to mine said data. Lastly, as touched on previously, unlike signature-based detection, anomaly-based detection is reliant on the technical expertise of the enterprises’ staff to function optimally (*Session 2: Network-Based Intrusion Detection*, 2022). Therefore, even if an alert is generated, it may be difficult for the security specialist/network administrator to understand if the activity in question is malicious (*Session 2: Network-Based Intrusion Detection*, 2022).

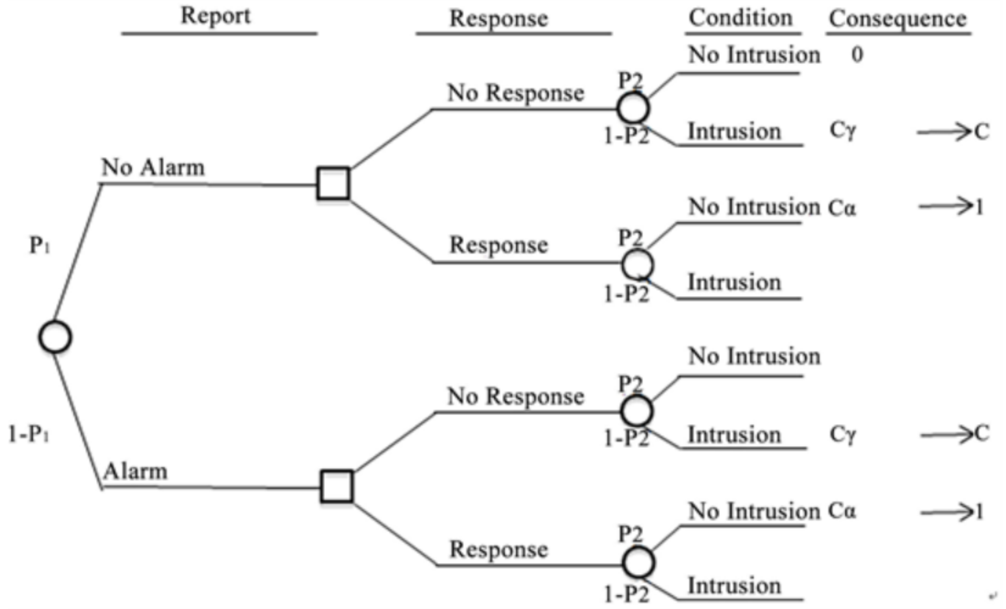
Hybrid NIDS

Ultimately, the solution to the relative weaknesses of both signature and anomaly-based NIDS has been to combine both detection methodologies into a hybrid architecture thereby creating a more comprehensive, and therefore more accurate, NIDS (Khraisat et al., 2019). Although, it must be noted that hybrid models retain the same concerns about the reliability/usefulness of the data sets they were trained and tested on (regarding their anomaly-based detection component) (Aldweesh et al., 2019). Additionally, the hybrid NIDS architecture also combines the costs associated with each approach to intrusion detection, and therefore while accurate, its cost is likely to be prohibitive for many organizations (*What Are the Pros and Cons of Signature-Based vs. Anomaly-Based Detection?*, n.d.). Therefore, the question of what NIDS deployment architecture is ideal for organizations that have limited resources to spend on network security remains.

Cost-Based Analysis of Intrusion Detection Accuracy

For starters, the ideal NIDS would have a 100% intrusion detection accuracy rating at the lowest possible cost (Imoize et al., 2018). However, if the cost required to get the closest to 100% intrusion detection accuracy is not feasible then how should an organization determine which NIDS deployment architecture to choose?

The answer to this question is to utilize “the principle of the Receiver Operating Characteristics” (Imoize et al., 2018) to assess the intrusion detection capabilities of a given IDS across its range of potential sensitivity configurations and then assign a value (cost) to all of the outcomes that result from their intrusion detection determinations (correct and incorrect) (Imoize et al., 2018). To that point, the "decision tree" (Imoize et al., 2018) mapping all situations relating to the expected costs of an IDS is listed below (Imoize et al., 2018).



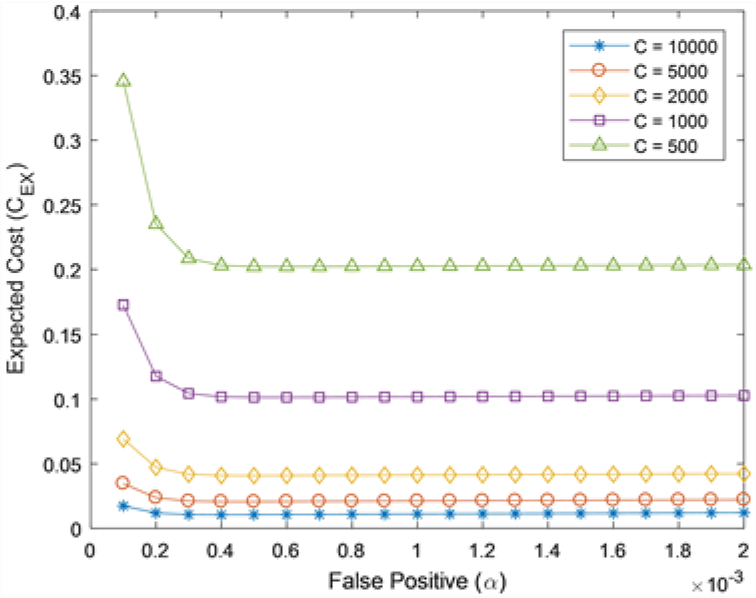
(Imoize et al., 2018)

As expected, the most costly situations are ones where the NIDS has incorrectly assessed the network traffic (false positive & false negative) (Imoize et al., 2018). Although, Imoize et al. (2018) find that changes in false positive rates (from NIDS) in networks with low occurrences of attempted intrusions have an even greater effect on the intrusion detection capability rating i.e., "CID" (Imoize et al., 2018), of a given NIDS compared to variations in the rates of false negatives (Imoize et al., 2018). The full formula for calculating an IDS' intrusion detection capabilities where "C_{ID} is intrusion detection capability, B is base rate, γ is false negative (FN) rate, α is false positive (FP) rate, PPV is positive predictive value and NPV is negative predicative value" (Imoize et al., 2018) is shown below (Imoize et al., 2018).

$$C_{ID} = \frac{-B\log B-(1-B)\log(1-B)}{-B(1-\gamma)\log PPV-B\gamma\log(1-NPV)-(1-B)(1-\alpha)\log NPV-(1-B)\alpha\log(1-PPV)}$$

(Imoize et al., 2018)

Ultimately, the study by Imoize et al. (2018) concludes that for a network with low occurrences of attempted intrusions, the key to minimizing costs while maximizing intrusion detection capabilities, i.e., the “optimal operating point” (Imoize et al., 2018) is achieved by limiting the occurrence of false positives. Although, it is worth noting that the benefit of limiting false positives, in terms of the IDS’ expected cost, quickly diminishes as more false positives are registered (Imoize et al., 2018). The following graph illustrates these findings (Imoize et al., 2018).



(Imoize et al., 2018)

As previously discussed there are some legitimate concerns with the data sets used to test many of the anomaly-based NIDS algorithms, and therefore, we will focus on an NIDS’ ability to correctly identify normal network traffic (Aldweesh et al., 2019). Moreover, while it is not feasible to review the accuracy of every NIDS, it is widely accepted that signature-based NIDS is less prone to false positives than anomaly-based NIDS (Khraisat et al., 2019). Therefore, a signature-based NIDS operating in a network with low occurrences of attempted intrusions is likely to offer a better return on investment compared to an anomaly-based NIDS (Imoize et al., 2018).

Conclusion

In conclusion, the most effective network intrusion detection systems contain both signature-based and anomaly-based intrusion detection capabilities, however, this is not a feasible NIDS deployment architecture for all organizations due to its cost (Khraisat et al., 2019; *What Are the Pros and Cons of Signature-Based vs. Anomaly-Based Detection?*, n.d.). Therefore, more nuanced evaluations of NIDS must be employed, i.e., the cost of the NIDS deployment architecture relative to the benefits it provides must both be weighed against one another.

To that point, it was illustrated previously how signature-based NIDS was a cheaper deployment architecture compared to anomaly-based NIDS (and hybrid NIDS) for several reasons (*What Are the Pros and Cons of Signature-Based vs. Anomaly-Based Detection?*, n.d.). One reason is the cost savings resulting from not having to employ/contract the highest-quality network security experts (*Session 2: Network-Based Intrusion Detection*, 2022). Furthermore, the signature-based intrusion detection approach does not require as significant computational resources compared to anomaly-based intrusion detection (Aldweesh et al., 2019). Moreover, the computational requirements gap between both approaches seems likely to worsen as there appears to be a positive correlation between the detection capabilities of anomaly-based NIDS and the complexity of the data mining techniques used (Aldweesh et al., 2019). Moreover, as for the costs associated with the intrusion detection capabilities of each approach, it was shown earlier that the way to limit the cost of a NIDS deployment (in a network with low occurrences of attempted intrusions) is to utilize a detection system that has the lowest occurrence of false positives (Imoize et al., 2018). To that point, signature-based NIDS does just that as it offers increased accuracy (fewer false positives) compared to anomaly-based detection (Khraisat et al., 2019). Therefore, for all the reasons just noted, a signature-based NIDS would be a more cost-effective deployment architecture than anomaly-based NIDS for enterprises operating a network with low rates of attempted intrusions.

References:

Abbasi, M., Shahraki, A., & Taherkordi, A. (2021). Deep Learning for Network Traffic Monitoring and Analysis (NTMA): A Survey. *Computer Communications*, *170*, 19–41. Sciencedirect. https://doi.org/10.1016/j.comcom.2021.01.021

Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J., & Ahmad, F. (2020). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Transactions on Emerging Telecommunications Technologies*, *32*(1). https://doi.org/10.1002/ett.4150

Aldweesh, A., Derhab, A., & Emam, A. Z. (2019). Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues. *Knowledge-Based Systems*, 105124. https://doi.org/10.1016/j.knosys.2019.105124

Comito, C., & Talia, D. (2017). Energy consumption of data mining algorithms on mobile phones: Evaluation and prediction. *Pervasive and Mobile Computing*, *42*, 248–264. https://doi.org/10.1016/j.pmcj.2017.10.006

Davis, J. J., & Clark, A. J. (2011). Data preprocessing for anomaly based network intrusion detection: A review. *Computers & Security*, *30*(6-7), 353–375. https://doi.org/10.1016/j.cose.2011.05.008

Fortinet. (n.d.). *What is the CIA Triad and Why is it important?* Fortinet. Retrieved July 4, 2023, from https://www.fortinet.com/resources/cyberglossary/cia-triad

Gyamfi, E., & Jurcut, A. (2022). Intrusion Detection in Internet of Things Systems: A Review on Design Approaches Leveraging Multi-Access Edge Computing, Machine Learning, and Datasets. *Sensors*, *22*(10), 3744. https://doi.org/10.3390/s22103744

IBM Data and AI Team. (2023, July 6). *AI vs. Machine Learning vs. Deep Learning vs. Neural Networks: What's the difference?* IBM Blog. https://www.ibm.com/blog/ai-vs-machine-learning-vs-deep-learning-vs-neural-networks/

Imoize, A. L., Oyedare, T., Otuokere, M. E., & Shetty, S. (2018). Software Intrusion Detection Evaluation System: A Cost-Based Evaluation of Intrusion Detection Capability. *Communications and Network*, *10*(04), 211–229. https://doi.org/10.4236/cn.2018.104017

Joshi, M., & Hadi, T. (2015). *A Review of Network Traffic Analysis and Prediction Techniques*. https://arxiv.org/ftp/arxiv/papers/1507/1507.05722.pdf

Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity*, *2*(1). https://doi.org/10.1186/s42400-019-0038-7

Larriva-Novo, X., Villagrá, V. A., Vega-Barbas, M., Rivera, D., & Sanz Rodrigo, M. (2021). An IoT-Focused Intrusion Detection System Approach Based on Preprocessing Characterization for Cybersecurity Datasets. *Sensors*, *21*(2), 656. https://doi.org/10.3390/s21020656

Otoum, Y., & Nayak, A. (2021). AS-IDS: Anomaly and Signature Based IDS for the Internet of Things. *Journal of Network and Systems Management*, *29*(3). https://doi.org/10.1007/s10922-021-09589-6

S, K., Wichers, Jkurucar, & kingthorin. (2020). *Intrusion Detection | OWASP Foundation*. Owasp.org. https://owasp.org/www-community/controls/Intrusion_Detection#:~:text=Once%20the%20system%20has%20a

Scarfone, K., & Mell, P. (2012). *Guide to Intrusion Detection and Prevention Systems (IDPS) (Draft) Recommendations of the National Institute of Standards and Technology*. https://csrc.nist.gov/csrc/media/publications/sp/800-94/rev-1/draft/documents/draft_sp800-94-rev1.pdf

Session 1: Introduction and Course Overview. (2022). UMGC. https://learn.umgc.edu/d2l/le/content/771160/viewContent/30758762/View

Session 2: Network-Based Intrusion Detection. (2022). Learn.umgc. https://learn.umgc.edu/d2l/le/content/771160/viewContent/30758763/View

Session 11: Output Plug-Ins and Operational Use. (n.d.). UMGC. Retrieved July 28, 2023, from https://learn.umgc.edu/d2l/le/content/771160/viewContent/30758774/View

Sourcefire. (n.d.). *Performance Rules Creation*. Snort-Org-Site.s3.Amazonaws.com. Retrieved July 26, 2023

Stallings, W. (2007, August 24). *Introduction to Network-Based Intrusion Detection Systems*. InformIT Database. https://www.informit.com/articles/article.aspx?p=782118

The OSI Reference Model Explained. (n.d.). Learncisco.net. Retrieved July 6, 2023, from https://www.learncisco.net/courses/ccna/part-1-internetworking/the-osi-reference-model.html

What are the pros and cons of signature-based vs. anomaly-based detection? (n.d.). Www.linkedin.com. Retrieved July 28, 2023, from https://www.linkedin.com/advice/0/what-pros-cons-signature-based-vs-anomaly-based