future internet

MDPI

Article

Cost Benefits of Using Machine Learning Features in NIDS for Cyber Security in UK Small Medium Enterprises (SME)

Nisha Rawindaran [1,2,3], Ambikesh Jayal [1,*], Edmond Prakash [1] and Chaminda Hewage [1]

[1] Cardiff School of Technologies, Cardiff Metropolitan University, Cardiff CF5 2XJ, Wales, UK; nisha@aytel.co.uk or nrawindaran2@cardiffmet.ac.uk (N.R.); eprakash@cardiffmet.ac.uk (E.P.); chewage@cardiffmet.ac.uk (C.H.)
[2] Aytel Systems Ltd., Cardiff CF3 2PU, Wales, UK
[3] KESS2, Knowledge Economy Skills Scholarships, Supported by European Social Funds (ESF), Bangor University, Bangor, Gwynedd LL57 2DG, Wales, UK
* Correspondence: ajayal@cardiffmet.ac.uk; Tel.: +44-029-2041-6395

Abstract: Cyber security has made an impact and has challenged Small and Medium Enterprises (SMEs) in their approaches towards how they protect and secure data. With an increase in more wired and wireless connections and devices on SME networks, unpredictable malicious activities and interruptions have risen. Finding the harmony between the advancement of technology and costs has always been a balancing act particularly in convincing the finance directors of these SMEs to invest in capital towards their IT infrastructure. This paper looks at various devices that currently are in the market to detect intrusions and look at how these devices handle prevention strategies for SMEs in their working environment both at home and in the office, in terms of their credibility in handling zero-day attacks against the costs of achieving so. The experiment was set up during the 2020 pandemic referred to as COVID-19 when the world experienced an unprecedented event of large scale. The operational working environment of SMEs reflected the context when the UK went into lockdown. Pre-pandemic would have seen this experiment take full control within an operational office environment; however, COVID-19 times has pushed us into a corner to evaluate every aspect of cybersecurity from the office and keeping the data safe within the home environment. The devices chosen for this experiment were OpenSource such as SNORT and pfSense to detect activities within the home environment, and Cisco, a commercial device, set up within an SME network. All three devices operated in a live environment within the SME network structure with employees being both at home and in the office. All three devices were observed from the rules they displayed, their costs and machine learning techniques integrated within them. The results revealed these aspects to be important in how they identified zero-day attacks. The findings showed that OpenSource devices whilst free to download, required a high level of expertise in personnel to implement and embed machine learning rules into the business solution even for staff working from home. However, when using Cisco, the price reflected the buy-in into this expertise and Cisco's mainframe network, to give up-to-date information on cyber-attacks. The requirements of the UK General Data Protection Regulations Act (GDPR) were also acknowledged as part of the broader framework of the study. Machine learning techniques such as anomaly-based intrusions did show better detection through a commercially subscription-based model for support from Cisco compared to that of the OpenSource model which required internal expertise in machine learning. A cost model was used to compare the outcome of SMEs' decision making, in getting the right framework in place in securing their data. In conclusion, finding a balance between IT expertise and costs of products that are able to help SMEs protect and secure their data will benefit the SMEs from using a more intelligent controlled environment with applied machine learning techniques, and not compromising on costs.

Keywords: network intrusion; intrusion detection; cybersecurity; cyber threat; machine learning; artificial intelligence; intrusion; detection; prevention; OpenSource

check for updates

Citation: Rawindaran, N.; Jayal, A.; Prakash, E.; Hewage, C. Cost Benefits of Using Machine Learning Features in NIDS for Cyber Security in UK Small Medium Enterprises (SME). *Future Internet* **2021**, *13*, 186. https://doi.org/10.3390/fi13080186

Academic Editor: Francesco Buccafurri

Received: 1 July 2021
Accepted: 15 July 2021
Published: 21 July 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Intrusion, detection, and prevention have always been three words that have resonated since the invention of the internet [1]. Many approaches towards these objectives have been used and trialed, and some have succeeded or failed, and others targeted, and broken. As technology advances, the need to secure data and protect them has changed. There is the continuous fear that an attacker trying to steal would always find a way around the secure lock, with or without a key.

The integration of real-world objects with the internet brings cybersecurity threats to most of our daily activities [1]. Technology and methods of communications have advanced since the start of the internet and as users learn to manage systems, users will look for more ways in which they can become more powerful and learn to distribute and share their data safely. With more wired and wireless connections and devices on the market, the problem of safety increases.

This study aims to look at how SMEs handle, store and protect their data using devices that are readily available in the market. With the current UK General Data Protection Regulation (GDPR) Act in operation, data storage has taken on a different dimension in its importance on how SMEs can keep safe. COVID-19 has also added to the mix of how vulnerable SME data can be due to the working environment changing from the security of the office to the vulnerability of the home network. The motivation for this study comes from various recent literature on how usage of machine learning could help make devices more robust in the way they are able to detect zero-day attacks and most important how much these devices cost. The research question explores the financial aspects of investing in devices that use machine learning technology in network devices to contribute towards the intelligence of detection, prevention, and protection of data. This is seen as useful for intrusions that are constantly hitting the SME networks, and takes a look at the vulnerability reflected in the current cyber pandemic alongside the real world COVID-19 status, and how much SMEs would need to invest in keeping their data safe and secure.

In this study, the devices chosen by the SMEs were specific in that they were able to detect and prevent any intrusions coming into the network. Various devices were taken into consideration for this experiment, and finally, as pre-mentioned, three choices were made for which devices were to be observed in this experiment in both the live data centre of the SME and the working network of the home office environment. The analysis will include an examination of the variety of these devices and models, in what is referred to as Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), that leads to IDPS, a combination of both devices in one. This study will then include a demonstration of how different vendors have been able to cope with technology and break the minds of "internet gang warfare", that is, the world of hackers. The final implications of this experiment will reflect on the cost and answer the question of "how much is this device, and will it protect my system?".

This study brings together the world scenario of the COVID-19 pandemic and its lasting effects on the birth of this cyber pandemic. It was during this study that the world became exposed to more prominent attacks currently leading the world such as Ransomware, Phishing, Malware, and social engineering amongst others. The realities of these threats have evolved into both technologies as well as wider policies towards managing threats. Protection of data as shown in this study is the reason why IDPS systems have come into force and are important within the SME market. Following on from this study, we can see a path in which where we could potentially bridge the gap between OpenSource code, such as SNORT and pfSense, and Commercial Network Intrusion Detection (NIDs) such as Cisco for further development.

The structure of this paper will start its journey by exploring the understanding of Big Data in Section 2 referring to Data Protection. Here, information on what users are trying to protect, why they want to protect it and how government policies and procedures can help in this process is discussed. Section 3 refers to Data and Information. Here, literature is explored on how data are managed and how different detection mechanisms are used.

These refer to various methods such as mathematical models, algorithms, and approaches of machine learning that will contribute to the implementation and success of an individual IDPS within a network or device of a business.

In Section 4, there will be a discussion of aspects of cyber threats and attacks. Section 5 then discusses research concerning governance and policy of Data Protection referred to as GDPR, in managing these threats in the public domain.

Section 6 discusses the role of hardware and software used in Data Protection, specifically how SME businesses use these commercial IDPS devices such as Cisco and OpenSource in this example, in a live environment. In this section technical research is explored in the choice of IDPS used in this study. Cisco devices are then compared to the OpenSource devices in a controlled experiment within a home and office network as discussed in the next sections. The discussion of machine learning and its techniques is also explored in this section.

Methodology in the evaluation of IDPS devices is discussed in Section 7, followed by the findings and analysis of each scenario given in this experiment. Section 7 will also focus on the cost models of how much these devices are a financial impact on the SMEs and its support of ML in the IDPS systems. Costs remain a focal point within this section on the financial impact is on an SME to keep their data safe.

Section 8 will see the conclusion and will answer the question posed in this study of how SMEs are able to detect zero-day attacks using machine learning techniques in both OpenSource and commercial, in their business solution and finding the balance of costs alongside it.

2. Research in the Area of Data Protection

To begin this paper, understanding what users are trying to protect is important. Content of emails, photos, company information, all needs to be stored safely and securely. Businesses including SMEs, tend to generate huge amounts of data on a daily basis [2]. In order to make sure that these data are kept safe and private, these businesses need to understand the importance of this protection. In order to do this, this study takes a look at the definition of Data and Big Data being used in general but paying specific interest to the SME market.

This section discusses the notion of Data and Big Data leading to the wide usage of devices in the pool of the Internet of Things (IoT).

2.1. Data and Big Data

"Data" and "Big Data" [2] through definition are the information that users key into the computer and store on the internet. These data can expand rapidly and exponentially, according to the amounts of digital information that are being generated. There are daily efforts for these data to be shared and analysed amongst SMEs to handle their data. The actual use of these data is to improve productivity, generate and facilitate innovation and improve decision making in SME companies working environment in the office or at home.

"Data" come from various sources, be it keying in numerical, graphical, or textual information, and then storing these data for future use, or archiving for reference. "Data" are small and manageable to handle whereas "Big Data" represent a higher volume of complex and linked data.

Gartner [3] defined "Big Data" as:

> " ... high volume, velocity and variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making."

"Internet of Things"(IoT) and people, tend to generate "Big Data". Cox and Ellsworth [4] were among the first to use the term "Big Data" referring to using larger volumes of data for visualization, datasets bigger than a "normal" dataset. Through time, businesses were not very good at keeping data intact or managing their data, and data input were as great as the data being output. The "Big Data" concept has now evolved to include a range of

characteristics, such as integrating different types of data and analyses. As IT facilities expanded, technology saw growth in more devices being introduced and connected to the internet so that they could access data freely. This was on an assumption that users had a good internet connection [2]. This is particularly important to the SME market in how they work and manage the expertise of their personnel and how they run their business. These networks of devices connected to the internet were raised in a study by Ashton [5] and provided the definition of this group of devices as the "Internet of Things"(IoT).

The term IoT was developed in 1999, and was initially meant to describe the following situation:

> "Today computers–and, therefore, the Internet–are almost wholly dependent on human beings for information. . . . The problem is people have limited time, attention, and accuracy–all of which means they are not very good at capturing data about things in the real world. . . . Users need to empower computers with their own means of gathering information, so they can see, hear and smell the world for themselves . . . " [4].

Data have since become much more than a dataset of information. Additionally involved is the rate at which these data can be processed and analysed and output to help with technology advancements in years to come. The statistics that lie behind these data become prevalent in how users move forward as technologists and how they can gain important information from analysing the data that are now readily available through the means of the internet [4].

In a study by Hernandez [6], it was stated that "Big Data" offered the opportunity to provide more information than traditional settings. In recent developments of "Big Data", the notion of trying to embed data into context was discussed. As an example, Hernandez explained that in the case of business transactions, new methods to store each transaction in the context of the SME business activity such as make payments, searches, or purchases, made it easier to generate reports and analysis of the data. By breaking the dataset into smaller fields or context, users could focus on individual information rather than bulk datasets. Hernandez also discussed how these data were able to show business owners how their business performed, who initiated various transactions, where customers and suppliers were located, and more audit trails through the concept of contextual datasets. The view of this expert then suggested that this information could therefore be processed through various means of theoretical structures or schemas and could facilitate the identification of the appropriate variables and the expected relationships between them. The data could then evolve into predicted values that could then help build the business to grow or stabilize. The data, according to this expert, were vital in steering the business in a positive direction. The management and development of Data and Big Data benefit SMEs and allow steady growth and progress of their business.

2.2. Internet of Things (IoT)

In the same study, Hernandez [6] discussed examples of IoT devices that help collate data positively in industry. An example of a sensor was given as an ideal IoT. Hernandez mentioned that sensors could include pacemakers, location identifiers, using the global positioning system (GPS), and individual identification devices, such as radio frequency identification (RFID) tags. Different information characteristics, typically of interest in the particular setting can be provided by sensors and may indicate time and location.

In a medical setting, pacemakers could capture information such as heart rate, status of the patients' vitals, what it is monitoring, the number of mobiles its applications have been downloaded to track and trace this particular patient and link this back to the hospital software for analysis. Many medical devices are able to also capture patient records, dates of illnesses and recovery information in line with various statistical models, perhaps to help develop vaccines to eradicate pandemics that could occur, in the example of COVID-19. These variables captured would require some consideration of the events, situations or settings of interest and current climate and speed of processing these data. With the

development of "Cloud" storage, this information then becomes accessible to anyone with the right permissions to work on these data moving forward from anywhere in the world.

This list of continuous monitoring of humans and social behaviors is non-stop, and data will continue to grow as there is no limit to the tracking and tracing of information and of course its storage. The sky is the limit or in this case, cyberspace. The next section explains how data is collected and managed and how IDPS starts to play an important role in its protection.

3. Data and Information

In this section, a study by Machanavajjhala [7] discussed data confidentiality, looking at analysis of how data are managed and how users intended to protect the data. It is said that a tremendous amount of data about individuals including their demographic information, internet activity, energy usage, communication patterns, and social interactions was constantly being collected by national statistical agencies, survey organizations, medical centres, and social networking companies [7]. The approaches discussed here argued that users had a problem when it came to ensuring the link between the privacy of the data against any relational data that a company privately or publicly held. For example, the use of social networks and how a large number of people were linked together through various social media platforms such as Facebook and Instagram. Through means of social media, it allows malicious actors to trawl public information, and gain information readily across the internet. In this way, data can be easily leaked out through individual people within the social media network. Malicious actors also choose to link people and information and obtain data over time [7]. Users are not aware of how the data are being distributed and used, and consequently also not aware of what information is made public or not. Users of social media tend to want to share topics and pictures freely, and easily thus forgetting the privacy issues that arise around this sharing. These users forget to look at their own privacy settings and fail to update them from time to time.

In data management, it is always useful to be aware of personal information and public personal information (PPI), and how social media and the internet translates to this. In a study by Iman, R.N et al. (2020), a different notion to the above was researched on user awareness and consciousness of personal information on social media and how these participants were aware of the scope of public personal information (PPI) [8]. The Iman study suggested that there was a concern for these social media users over the potential misuse of their personal information and data, which is closely related to individual privacy. Further, Iman adds to the policy perspective of the UK General Data Protection Regulation (GDPR) which defines personal data as any information relating to an identified or identifiable natural.

Data of this nature need management. According to Gartner [3], data management:

> "...consists of the practices, architectural techniques, and tools for achieving consistent access to and delivery of data across the spectrum of data subject areas and data structure types in the enterprise, to meet the data consumption requirements of all applications and business processes."

Technologists and inventors build tools to help society manage data and share data that are input into the internet. With the help of technology giants such as Microsoft, Apple, IBM and Cisco to name a few, there is a choice of tools and environments to make day-to-day management of data, easy and manageable. Through this infrastructure, these tools with the right software and devices around it, allow various levels of access and protection depending on the nature of the data being managed. The awareness of users utilising these devices is equally important in this management of data.

The more connected to the internet society becomes, the more "back doors" are potentially opened. Malicious actors will always find a way to gain access to data they can sell on. This can leave data vulnerable in terms of others getting hold of it and how the malicious actors can take it. In practice, it is not possible to build a completely secure system. Sundaram [9] explains that the internet is changing methods of computing rapidly,

and possibilities and opportunities for malicious intrusions are very high and can cause high risk. Security mechanisms of a system are designed to prevent unauthorized access to system resources and data, however complete protection is unrealistic in this fast-paced cyber world users are in.

In a recent survey, Sardi, A. et al., (2020) showed that since the beginning of the COVID-19 pandemic, the World Health Organization (WHO) had detected a dramatic increase in the number of cyber-attacks. An alarming result came from Italy [10] in which the COVID-19 pandemic had heavily affected cybersecurity from January to April 2020. The total of attacks, accidents, and violations of privacy had doubled due to the detriment of companies and individuals shifting from various securities locations within their country. Sardi, A. et al., further explored the various devices that were used during the pandemic to affect security.

As hackers become increasingly clever and the uses of bots [11] take over, their "attacking" methods rely on Machine Learning (ML) techniques which is a subset of Artificial Intelligence (AI) to help. Bots is a short form for "Virtual Robots" that are programmed to use malicious code [11]. Bots are highly adaptable worker bees that do their masters' bidding over a broad internet, in this case, robots scattered throughout the global internet. There exist both good bots and bad bots, it all depends on how they are used. Through this study, the observation looks at various methods to help devices identify these bots and how they behave. In order to keep up with these hackers and their bots and monitor their activities, the use of an IDPS system is now even more important than ever [1]. An IDPS system is able to help learn about bad patterns compared to good patterns on the internet. These various approaches are needed to protect and shield our data, big and small.

The following section will raise awareness of cybersecurity and its threats towards handling and protecting Data and Big Data. The types of threats and their preventions are discussed.

4. Cybersecurity and Its Threats

In a paper presented by Gallaher, cybersecurity refers to:

> "a measure for protecting computer systems, networks, and information from disruption or unauthorized access, use, disclosure, modification or destruction" [12].

With it follows threats. The paper goes on to define cybersecurity threats as:

> "Asymmetric, surreptitious and constantly evolving–a single individual or a small group anywhere in the world can inexpensively and secretly attempt to penetrate systems containing vital information or mount damaging attacks on critical infrastructure" [12].

There are various sources of malicious actors. They can range from insider threats, general hackers, low-level unorganized criminals, terrorists, insurgents, organized criminal networks, machines, bots amongst many more. The type of attacks carried out can also range from distributed denial of service (DDoS), data destruction, espionage, state commercial, theft, and hacktivism. These attacks are usually a target for governments, business industries, defense, law, security, infrastructures, industries, individuals, and many other citizens around the world [11]. The next section discusses the top four types of cyber-attacks.

4.1. Top Four Attacks

In a recent research study by Preuveneers, D. and Joosen, W., (2021) [13], cyber threat intelligence is important to validify the various threats that exist on the internet. Understanding these threats allows collaboration efforts between organisations in helping them better understand these types of attacks allowing businesses to proactively defend their systems and networks from cyber-attacks. Some of the top attacks currently leading

the world are the likes of Ransomware, Phishing, Malware, and Social Engineering amongst others. These identified attacks are discussed below.

4.1.1. Ransomware

Ransomware, in their first report published in 2015, the Cyber Threat Security Alliance (2015) [14] introduced the following definition of ransomware. They said that,

> "Ransomware is a type of malware that encrypts a victims files and subsequently demands payment in return for the key that can decrypt said files. When ransomware is first installed on a victim's machine, it will typically target sensitive files such as important financial data, business records, databases, personal files, and more. Personal files, such as photos and home movies, may hold sentimental value to the victim."

Ransomware is designed to extort money, blocks access to files until a ransom is paid, deny access to files until, or threaten to publish the victim's data unless a ransom is paid (although there is no guarantee that access will be restored, or that the criminal hacker will destroy the data).

4.1.2. Phishing

Phishing is a form of online identity theft that aims to steal sensitive information such as online banking passwords and credit card information from users. One definition of phishing is given as,

> "a criminal activity using social engineering techniques" [15].

Phishers attempt to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication [15].

4.1.3. Malware

Malware is a general label for malicious software that spreads between computers and interferes with computer operations as described by McGuire [16]. Malicious software is designed to gain unauthorised access to cause damage. Malware can be deemed destructive, for example, deleting files or causing system crashes and stealing personal data. An example of malware includes viruses.

Viruses can cause computer dysfunction but can also have more severe effects in terms of damaging or deleting hardware, software, or files. Viruses are self-replicating programs and can spread within computers. They require a host (such as a file, disk, or spreadsheet) in a computer to act as a carrier, but they cannot infect a computer without human action to run or open the infected file.

Another example of malware, according to McGuire [16] is worms. Worms are also self-replicating programs, but they can spread autonomously, within and between computers, without requiring a host or any human action. The impact of Worms can therefore be more severe than Viruses, causing destruction across whole networks. Worms can also be used to drop Trojans onto the network system.

Trojans are a form of malware yet again, that appear to be legal programs but facilitate illegal access to a computer. They can perform functions, such as stealing data, without the user's knowledge and may trick users by undertaking a routine task while actually undertaking hidden, unauthorised actions.

4.1.4. Social Engineering

Social engineering, also known as human hacking, is the art of tricking employees and consumers into disclosing their credentials and then using them to gain access to networks or accounts as raised by Conteh [17] in their study. In an article written by McCarthy [18], there were three basic types of tactics discussed that were currently being

used to manipulate humans in getting information out of them. In the study, the three types are shown below.

I. In-Person: Human-to-human interactions resulted in 63% of data breaches from internal sources.
II. Phone: 4.6 million phone calls were made, and information attacks carried out in 2013.
III. Digital: 77% of attacks were phishing.

McCarthy went on to discuss that there was a fine balance of trust and suspicion through personal interaction. When allowing trust to build between strangers, this gave access to malicious individuals to take advantage of the blind trust. By recognising certain warning signs, users were made more aware of their surroundings. There were various ways in which users overcome the above tactics and become more aware of whom they were dealing with.

From the above top four types of attacks currently floating on the internet, it is without a doubt that there are many factors that will need to be investigated in how our society moves forward in a safe cyber world. Within this domain of cybersecurity and threats, this paper will continue to focus on the specific approaches towards managing these within the public institutional domain.

4.2. Research on Attack Prevention

There are several factors that need consideration that can prevent the attacks of social engineering and the other forms of attacks, from recurring. Amongst them are the consideration of creating an incident response team to monitor the phone calls and incidence that happen in businesses and SMEs in particular. The extensive use of encryption, employee training, and business continuity plans is amongst other measures to consider. Insurance protection and board-level engagement are vital for the protection of staff using the internet.

Before any investigations are to be carried out on how data are protected from the identified malicious actors, the next section defines a policy that was introduced back in May 2018. This policy has changed the face of how the UK and Europe as a combined region of nations, handle data and how collectively united these countries are in choosing the Act to protect its data. This policy framework, known as General Data Protection Regulation (GDPR) act, will be discussed and will then be followed by showing the technologies that are involved in data protection [19].

5. Governance and Policy on Data Protection

General Data Protection Regulation (GDPR) as it applies in the UK and EU nations, was facilitated in the UK by the Data Protection Act 2018. The General Data Protection Regulation is a Europe-wide law that replaced the Data Protection Act 1998 in the UK. It places a greater obligation on how organisations handle personal data. It came into effect on 25 May 2018 [19].

The GDPR applies to "personal data" and since its introduction, businesses and organisations have had to follow a new way of working in order to make sure data are safe and protected. With the introduction of GDPR, the UK government through its surveys has recognised a drop in personal information being misused.

Global threat has taken a public profile and concerns people in all aspects of life and businesses and has become of relevance in policies. In order to take this forward, the section will discuss the wider definition of the theories of data protection and their approach towards rules and safeguards that have emerged through surveys and facts that have been collected in the past few years.

As is known to the public, there has been a rise in cyber-attacks with public bodies such as the National Health Service (NHS), BUPA, EasyJet, and British Airways to name a few, that have seen their data being breached, stolen, ransomed, and other varieties of attacks displayed on them. The Information Commissioner's Office (ICO) governing body

has been able to act and penalise these organisations based on the GDPR policies and has made these organisations tighten their own internal policies and procedures and take the importance of IT to the front burner of their organisation [19].

In a recent news coverage by the BBC on EasyJet, May 2020 [20], it was reported that a "highly sophisticated cyber-attack" had affected approximately nine million customers' data. It was understood that the hackers stole credit card data including the three-digit security code, known as the Card Verification Value (CVV) number, on the back of the card itself. Following from a case like this, the ICO plays an important role in making sure the policies of GDPR were followed and people's right to know that an organisation as big as EasyJet handled their data appropriately, securely, and responsibly.

In another report by the BBC, ransomware was the method used in an attack on the NHS back in 2017 [21]. NHS Digital said the attack was believed to have been carried out by the malware variant Wanna Decryptor. The NHS is a huge organisation thus having many providers supporting their IT infrastructure and core network. The BBC reported that "Complexity is the enemy of security" and went on to emphasise that some networks could have benefitted from updated security patches and computers upgraded to stop the cyber threat from occurring. This led to hackers being able to easily penetrate the network of the NHS and cause disruption and financial loss.

According to CSO Online [22] Cyber Attack Statistical Report March 2020; showed eight key cybersecurity statistics at-a-glance:

I. 94% of malware is delivered via email.
II. Phishing attacks account for more than 80% of reported security incidents.
III. 60% of breaches involved vulnerabilities for which a patch was available but not applied.
IV. 63% of companies said their data were potentially compromised within the last twelve months due to a hardware- or silicon-level security breach.
V. Attacks on IoT devices tripled in the first half of 2019.
VI. File-less attacks grew by 256% over the first half of 2019.
VII. Businesses will fall victim to a ransomware attack every 11 s by 2021.
VIII. 83% of respondents experienced a phishing attack in 2018.

The statistics above clearly show that businesses need to follow guidelines of GDPR, ICO and Cybersecurity. It also highlights the need to create procedures in place in order to make sure systems are up-to-date, and that hardware and software are monitored according to Cybersecurity standards set by government bodies in line with policies and procedures of the individual countries.

The Department of Digital, Culture, Media and Sport of the UK carried out a survey to collect data on Cybersecurity Breaches Survey 2019 covering 2018 and 2019, respectively [23]. This was a government initiative, and the survey that was carried out was to see how GDPR and Cybersecurity plans had made a difference to businesses and charities sectors.

An extract from the report, as shown in Figure 1 below, shows the relevance of GDPR and how its effects have shown the reduction in breaches over the course of the two years. Figure 1 shows the experience of breaches or attacks and the difference GDPR and Cybersecurity have made within organisations between 2018 and 2019.

Figure 1 above also shows that 32% of businesses identified cybersecurity breaches or attacks in the last 12 months. It also explains the GBP 4180 was the average annual cost for businesses that lost data or assets after breaches. The report went on to further show that amongst the 32% that suffered these breaches, 32% needed new measures to prevent future attacks, 27% took up staff time dealing with breaches or attacks, 19% had staff stopped from carrying out their daily work and 48% identified at least one breach or attack a month.

Figure 2 below shows the impact of the UK government's initiative of General Data Protection Regulation (GDPR) and the Information Commissioners Office (ICO), government official organisation contributed to the reduction in these breaches compared from 2018 and 2019.

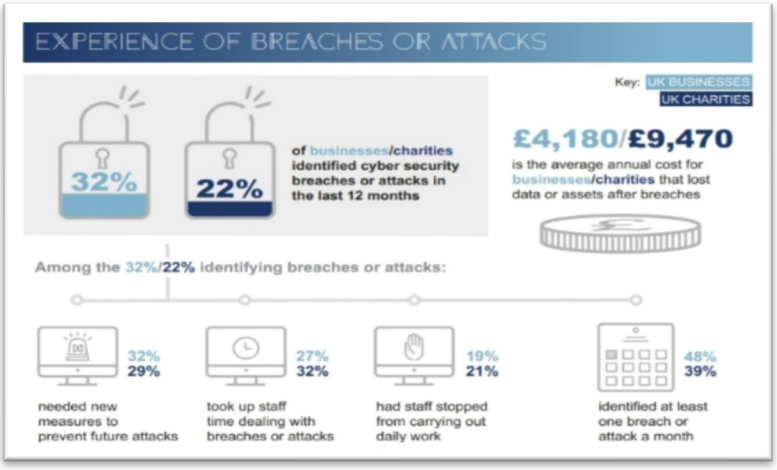

Figure 1. Cyberscurity Breach Survey 2019, Department of Digital, Culture, Media, and Sports UK [23].

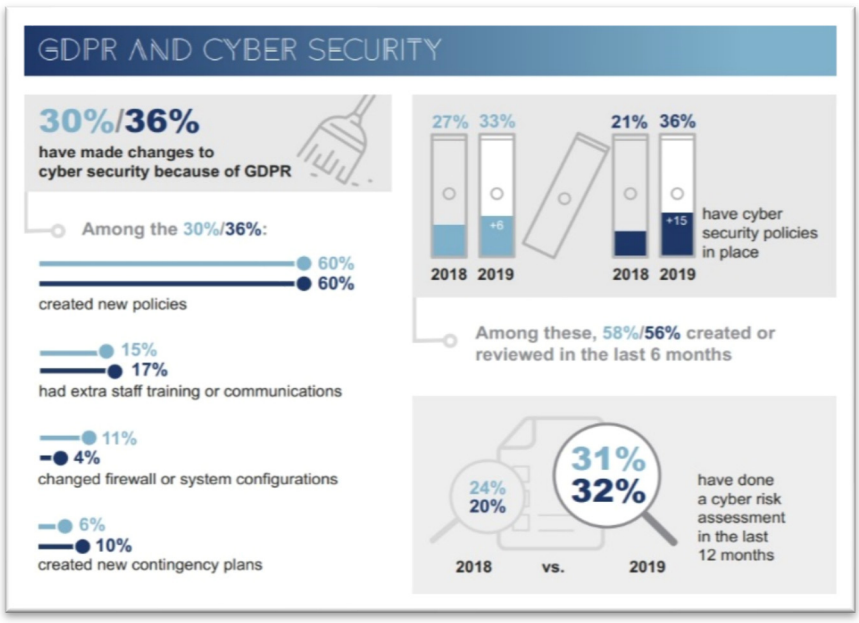

Figure 2. GDPR and Cybersecurity [23].

The statistics above in Figure 2 show that 30% of businesses made changes to their cybersecurity because of GDPR. From those companies, 60% implemented new policies, 15% had extra staff training or communications, 11% changed their firewall or systems configurations, and 6% created new contingency plans if they had another cyber-attack.

The year 2019 showed an increase in cybersecurity policies in place after GDPR was initiated through the government initiative. GDPR certainly gave businesses the platform to conform to standards and the ability to understand what protection was required to keep their data safe. This report showed that in 2019, more businesses than before had taken positive steps to improve their cybersecurity. This is in part linked to the introduction of GDPR.

Another importance of security and its best practices within SMEs and bigger organisations, is its compliance to varying standards and practices. Such examples are Cyber Essentials, Cyber Essentials Plus and International Standard for Information Security as referred to as ISO27001 and ISO27701, all of which give companies a means to protect and comply with the laws [23]. The SME in this paper complies with the UK rules and must observe the renewal of its certification every year to show its customers that it complies

with GDPR and UK standards. These best practices enable businesses to protect their assets and comply with UK laws and regulations.

A conference paper by Rawindaran, N. et al. (2020) showed how developed countries had created standards and implemented policies compared to developing nations. It was concluded that without a national strategy and responsibility at senior level authority, all cybersecurity activities were limited and deficient unless brought up to international standards [24]. Countries like the UK and other EU nations have a more consistent approach to cybersecurity and international cooperation in cybersecurity matters. Another example was the Netherlands, through their National Cybersecurity Council collaborating with other countries to strengthen its international orientation. Rawindaran et al. also discussed that some countries had a higher level of maturity than others when dealing with cybersecurity, cyberspace and policy making-strategy and its application. These leading countries recognise the importance of its achievements and advancement and come into an alliance to fight cybercrime and perform a level of knowledge transfer through the means of these standards and best practices [24].

By following guidelines and introducing a policy by law, a business is able to make an informed decision and operate in a safe and secure way in order to protect the data they manage. In the next section, the discussion will focus on how to apply detection and protection to data. Hardware and software devices are analysed and discussed as to how they play an important part in managing GDPR and Cybersecurity.

6. Hardware and Software for Data Protection

Through the years in the UK, large Internet Service Providers (ISPs) such as BT and Virgin Media have partnered with large international network supplier vendors such as Microsoft, Cisco, Dell, HP, and others, to create networks and devices to help increase the safety of its boundaries and keep data protected. These vendors continuously work with technologists to improve the way in which this software and devices manage traffic and identify threats that are continuously evolving. These software and devices have also helped increase security standards and have revolutionised the environment in which users navigate. They have created a defined space in which end-users can safely and securely work and protect their data and be able to operate.

UK businesses have adhered to global standards in which they can work under best practices to ensure their information is protected and guarded against cyberattacks and other threats in the industry. Countries are starting to understand cybersecurity terminologies and the threats that skirt around this space, and have been able to provide businesses the safety and protection they require in order to protect the data they work in. Introducing GDPR and Cybersecurity in the UK, have improved business practices at the management level assisted by key players in the IT industry. This involvement by higher management has allowed networks and security to get in line with the National CyberSecurity Centre (NCSC), another official government regulatory body in the UK. IT companies in the UK who provide infrastructure to house customer data have had to lean on enterprise solutions such as Cisco and HP for their state-of-the-art firewalls and network intrusion detections/prevention systems, to make sure these attacks do not re-occur and/or are constantly monitored via guidance from the headquarters of these multivendor suppliers [24].

From this, industries have had to lean on vendors for hardware devices and software applications as a method of catching up and identifying new behaviour and strains of viruses and other threats over the internet. Many anti-virus companies can only decode the software and thus their rate of recovery depends on the code and software being used. Using vendor technology and their financial backing on how to create smarter applications, will speed up processing power and work alongside standard rules, helping scientists to develop programs that can predict an attack before it actually happens. This way of behavioural modelling will give machines the ability to hear the hacker before the machines can see the hacker. Developers sometimes fault in this area as nearly all companies want to

be the first to market rather than produce a device that is intelligent enough to take control and be the leaders in intrusion detection and prevention.

In a study by Global Market Insight [25], the Intrusion Detection and Prevention System (IDPS) market is predicted to hit USD 8 billion by 2025. Europe is seeing this market increase due to public–private partnerships and government investments to deploy the intrusion detection and prevention system in various points of the network system. The study goes on to describe this increase due to the market growth attributing to factors including the growing number of IT data breaches and security threats, rising demand for enterprise mobility, and stringent regulations established by the government to safeguard consumer data. The study also suggests that on average, over one million new types of malware are created by malicious actors each day. These types of malware try to infiltrate networks increasing the threat of network attacks, driving the usage and demand for the global IDPS market. The IDPS solutions monitor the working of firewalls, routers, files, and key servers in the network and send appropriate notifications and alarms on detecting a breach within the network, helping operators to establish and implement effective controls. Therefore, it is necessary to secure the supply chain when it comes to improved cyber hygiene.

OpenSource platforms are widely used within industry. The OpenSource definition is a bill of rights for the computer user as cited in Perens, B., (1999) [26]. Statistically, in a 2015 study as cited online by zdnet.com, 78% of companies run part or all of their operations on OpenSource and 66% create software for customers built on OpenSource. This has almost doubled since 2010 and will continue to grow exponentially according to this study. A major concern that follows this growth is the online management of the OpenSource code and its updates [27].

The following order will discuss how IDPS becomes a focal point of this paper's discussion on the type of hardware and software that is available in the market to detect attacks and consequentially prevent them from spreading.

6.1. Intrusion Detection and Prevention System (IDPS)

In a technical report presented by Anderson, J.P., (1980) [28] on Intrusion Detection, it was quoted that intrusion detection can be defined as,

> "An intrusion attempt or a threat to be the potential possibility of a deliberate unauthorized attempt to access information, manipulate information, or render a system unreliable or unusable."

It was in the late 80 s the famous incident of the Internet Worm of 1988 [24], that was made a highlight that operating systems and application programs could get hacked. It was during this same time there was discussion that computer network systems should provide confidentiality, integrity, and assurance against denial of service (DoS) in which the attacker fully breaks down the victim's network connectivity [29].

Due to the internets' increased usage and connectivity and the financial greed of individuals, intruders became more favourable to wanting to attack these systems. These intruders understood the ease in which the playing field of the internet was not protected therefore making it easy to attack if the hacker knew what they were doing. Back in the days of the infancy of the internet, data were never taken seriously, as no one could ever predict what the future held for the use of the internet and its data.

As decades and technology advanced, industry became clever, and companies started producing Intrusion Detection Systems (IDS). An IDS according to Teodoro, G. (2009) is able to detect any attacks on a system (preferably in real-time) and take appropriate action. An IDS does not usually take preventive measures when an attack is detected; it is a reactive rather than pro-active agent. It plays the role of an informant rather than a police officer [30]. Traditional methods of logging incidents involve that of audit data generated by the operating system and an audit trail to record these activities on a system. They are then documented in chronological order. Manual inspections were then conducted on the data produced via these audit trails to produce results. Engineers would then try and

locate the perpetrators and shut their activities down. As data rose exponentially, manual inspections were no longer feasible, hence automated IDS systems became favourable to detect these activities.

6.2. IDS Framework

Teodoro, G., (2009) [30] also went on to explain a framework created by DARPA (Defence Advanced Research Project Agency) called" Common Intrusion Detection Framework", a working group that was set up in 1998 to define a common framework in the IDS field. Integrated in 2000 and having adopted the new acronym IDWG ("Intrusion Detection Working Group"), the group defined a general IDS architecture based on the consideration of four types of functional modules. In the article, this framework is explained in the adaptation in the form of Figure 3 below.

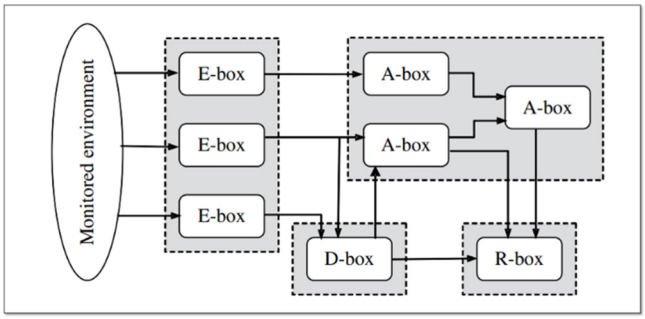

Figure 3. Adaptation of the IDS framework [30].

Figure 3 above provides the adaptation of the model for the IDS framework. The E blocks represent event boxes, and this contains sensor elements that monitor the target system, thus acquiring information events to be analysed by other blocks. The D blocks represent the Database-boxes. These are elements intended to store information from E blocks for subsequent processing by A and R boxes. A blocks are Analysis-boxes, and they are used for processing modules for analysing events and detecting potential hostile behaviour. From this, an alarm will be generated if necessary. The R blocks are the Response-boxes. The main function of this type of block is the execution, if any intrusion occurs, of a response to hinder the detected attacker as explained in this article.

IDS is able to track in real-time as well as perform post-mortem analysis of the extent of any damage caused by attacks. An IDS system leans heavily in the way businesses work and how they operate. These IDS systems also follow GDPR and Cybersecurity policies that enable the protection of data from losses against malicious actors trying to take these data. In the next subsections, different types of IDS are observed and how these systems contribute to analysing the network and its approaches in order to learn the various behaviours of malicious actors online.

6.3. Types of IDS

In this section technical securities behind IDS are explored, and how these are applied and used in the network for patrolling and detection of threats. A study produced by the National Institute of Standards and Technology (NIST) back in 2007 recognised the uses of the Intrusion, Detection and Prevention Systems (IDPS) as a way of identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators [31]. Businesses and organisations could also use IDPS as a means of identifying problems with security policies, documenting existing threats, and deterring individuals from violating security policies. This study gave insight into the characteristics of IDS and how to design, implement, config, secure, monitor, and maintain them plus offering the extension of a protection system. They offered a guideline and benchmark to administrators on how to maximise the usage of IDS. This IDS provides a new layer of

security in existing networks of computers and data and encouraged hardware vendors such as Cisco and HP to design fully integrated IDPS systems to do that and more [31].

Previous technology prior to IDPS, used Firewalls as a method of controlling traffic in and out of networks. Firewalls used a set of rules and followed them. An example of a firewall that is used in the SME business in this study is the Cisco 5520 device [32]. A device like this would usually sit in network topology and provide a layer of security that works on static rules where it permits and denies connections. It prevents intrusions and limits access based on the rules it is given. It never deviates from the rules as it operates in positive and negative, unable to think outside the box. This "normal" firewall acts as a single point of entry, green to pass and red to deny. Figure 4 below shows the basic firewall configurations in a network topology based on the authors drawing of the SME business in this study.

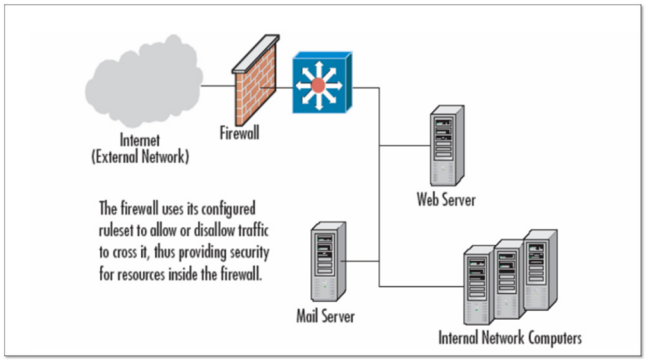

Figure 4. A basic firewall topology (Author's interpretation of SME business network).

Figure 4 above shows that the internet is an external network that needs to be protected by the firewall. The firewall uses its configured rule book to allow or disallow traffic to cross it and thus providing security for resources inside the firewall such as emails, shared folders, and internal network of computers.

Firewalls have simple rules to either allow or deny protocols, ports, or IP addresses. Some DoS attacks are too complex for today's firewalls. For example, if there was an attack on port 80 (web service), firewalls cannot prevent that attack because they cannot distinguish good traffic from DoS attack traffic [33].

Just as the hackers have evolved in their hacking threats, firewalls have also evolved in their technology. As time evolved and threats became complicated, the introduction of IDPS has become ever more important in its role in a network topology.

6.3.1. Network IDS and Host IDS

Accordingly, to the Open Systems Interchange (OSI) seven-layer model [34], understanding where the network topology lies is important. In a research article presented by Kabiri, there exist two types of IDS. They are Network IDS and Host IDS. The Network IDS is able to monitor incoming network traffic and the Host IDS is able to monitor the operating system machines and is able to take snapshots of machine files and tell the difference if anything changes [35].

Network IDS has an edge of importance as it is able to give coverage in detection across the entire network whereas the Host IDS is specific to the machine, its host. According to Cisco documentation [32], the definition of a Network Intrusion Detection System (NIDS) is as follows:

> "The goal of intrusion detection is to identify unauthorized use, misuse, and abuse of computer systems by both system insiders and external penetrators." [32]

Cisco reiterates that the intrusion detection problem is becoming a challenging task due to the heterogeneous computer networks since the increased connectivity of computer systems. This gives greater access to outsiders and makes it easier for intruders

to avoid identification. Intrusion detection systems (IDS) are based on the beliefs that an intruder's behaviour will be noticeably different from that of a legitimate user and that many unauthorized actions are detectable as stated in the paper by Mukherjee, B., (1994) [36].

The paper of Kabiri, P., (2005) [35] explains that the concept of IDS works on the theory of kernels. The kernel is responsible for classifying IDS into two groups namely normal and anomaly.

Normal is often referred to as Signature-Based Detection whereby IDS is able to recognise bad patterns of malware and anomaly is Anomaly-Based Detection where the IDS is able to identify any deviations from good traffic via Machine Learning.

Complementing the IDS is of course the Intrusion Prevention Systems (IPS) and how it acts as a management centre for the detection. IPS is able to describe the suspect intrusions, sound alarms, watches for attacks that originate from within the system, studies signature patterns and is able then to terminate connections and offer access controls. In the next sub-section, a closer look at the normal group detection called Signature-Based Detection is examined.

6.3.2. Signature-Based Detection

Signature detection is normally detected by their misuse and this method uses recognised patterns of unauthorized behaviour to predict and detect subsequent similar attempts. These patterns are called signatures [37]. For host-based intrusion, detection, and prevention, one example is "three failed logins." For network intrusion, detection and prevention, a signature can be as simple as a specific pattern that matches a portion of a network packet. For instance, packet content signatures and header content signatures can indicate unauthorized actions. The occurrence of a signature might not actually be attempted unauthorized access, it could just be an honest mistake. These systems are not unlike virus detection systems, they can detect many or all known attack patterns, but they are of little use for as yet unknown attack methods. The main advantage of the misuse detection paradigm is that it can accurately and efficiently detect instances of known attacks. The main disadvantage of misuse detection methods is that it lacks the ability to detect the newly invented attacks. Signature databases must be constantly updated, and IDS must be able to compare and match activities against large collections of attack signatures [37]. The next sub-section goes on to look at anomaly detection called Anomaly-Based Detection.

6.3.3. Anomaly-Based Detection

Anomaly detection is designed to uncover abnormal patterns that deviate from what is considered to be normal behaviour, whereas IDS establishes a baseline of normal usage patterns and anything that widely deviates from it gets flagged as a possible intrusion. An example of this would be if a user logs on and off of a machine eight times a day instead of the normal one or two. Additionally, if a computer is used at 2:00 a.m. when normally no one outside of business hours should have access, this should raise some suspicions. Anomaly detection can investigate user patterns, such as profiling the programs executed daily. Once again, if a user in an IT department suddenly starts to access accounting programs or recompiles them, then the system must immediately raise an alarm or alert its administrators. The major benefit of anomaly-based detection methods is that they can be very effective at detecting previously unknown threats [37].

Through the idea and introduction of Machine Learning in the anomaly detection system, in the first stage of a deployment of an anomaly-based IDS, the system learns what constitutes normal behaviour. The controlled system is running as usual under the assumption that there are no abnormal behaviours. During the learning stage, no attack must occur in the controlled system so that the IDS does not learn to ignore the attacks. The learning process can be addressed by a variety of means such as Machine Learning or building statistical behavioural profiles.

In the second stage of the deployment, in which the system possibly faces attacks, the IDS monitors the activities in the controlled system and compares them to the learned normal behavioural patterns. If a mismatch occurs, a level of "suspicion" is raised with the IPS and when the suspicion, in turn, trespasses a given threshold, the system triggers an alarm. The main advantage of anomaly detection is that it does not require prior knowledge of intrusion and can thus detect new intrusions. The main disadvantage is that it may not be able to describe what an attack is and may have a high false positive rate.

One other such research by Injadat, M., et al. (2020), to deal with more concise training data using more current datasets such as CICIDS 2017 and the UNSW-NB 2015 datasets (more recent to DARPA, as mentioned earlier), proposes a novel multi-stage optimized ML-based NIDS framework. According to this study, this method reduces computational complexity while maintaining its detection performance. The model results showed a significant reduction in the required training sample size. Detection accuracies were over 99% for both datasets, outperforming recent literature works lowering false alarm rates [38].

The next sub-section goes deeper into the algorithms that are used in the modelling of the detection methods.

6.3.4. Machine Learning

Within Machine Learning technology, there exist many datasets that are available on the internet for public usage [39]. Specific reference to one called KDD99 was first created in 1998 and last updated in 2008 and is one of the most known datasets in academic literature. There are many algorithms that have been trialed and tested under a supervised laboratory approach such as Support Vector Machine, Bayesian Network, Artificial Neural Network, Decision Tree, and k-Nearest Neighbour. According to Brown et al., one reason which machine learning algorithms are useful is the way decryption is performed and how they benefit real-life applications as modelled in Brown's paper [39]. Varying algorithms within Machine Learning are inspired by nature as these can provide a useful way of looking at a particular problem. Hewage, C. (2018) [40] paper describes nature-inspired algorithms to be employed to achieve solutions to difficult tasks. These algorithms come with advantages and disadvantages. The biggest advantage of these types of varying approaches from lab developed to nature-inspired, is that they recognize well-known malicious activities with high accuracy and low false alarm rate. The disadvantage of these types of approaches is that they have a weak recognition capability of zero-day attacks.

Using the right dataset is important for ML to increase its accuracy whilst reducing processing time. New datasets such as New Selected Learning-Knowledge Discovery in Databases Dataset (NSL-KDD) offer a much more impressive level of Big Data collected which influences the result of these anomalous detections. A study by Belgrana, F.Z., (2021) [41] implemented the Condensed Nearest Neighbors (CNN) algorithm as their approach using the classification and regression methods in a supervised learning method to analyse the distribution of samples. CNN reduced the data vector dimensions used and was able to utilise low consumption of system resources as well as a reduction in processing time while maintaining good detection results. Neural Network (NN) was also studied as a pre-classification of learning dataset to compare with another method being K Nearest Neighbors (KNN). The results showed that these approaches of IDS improved the detection rate, decreasing missed attacks while reducing processing time.

Continuing approaches in supervised learning techniques of ML follow the research of Di Mauro, M., et al. (2021). Their study recognised that dealing with the vast diversity and number of features that typically characterize data traffic is a challenge. Therefore, their paper addressed issues such as the presence of several features leading to lengthy training processes particularly when features are highly correlated. The second issue is where bias was introduced during the classification process of a supervised learning method. Their research paid particular importance to Feature Selection (FS) pre-processing steps in network management and, for network intrusion detection [42].

In an unsupervised approach, the dataset used does not contain any class information. It is based on an assumption model and that being the user profile of the attacker cannot change in a short time and malicious activity causes an abnormal change in the network, as explained in an article blog in normshield.com [40]. In this unsupervised state, an algorithm called operational logic is used to create these assumed classes of malicious actors and abnormalities via web browsing and email traffic. These classes can either have a huge event count or an extremely small event count. The advantage here is the ability to detect zero-day attacks. The disadvantage is that the attacker can produce network traffic intelligence enough to bypass the IDPS systems and execute a high false alarm.

Di Mauro's research mentioned earlier gave useful insights to network and security managers of businesses who are considering the incorporation of ML concepts into network intrusion detection, where trade-offs between performance and resource consumption are crucial [42].

Signature-based approaches are very good at identifying attacks that are well known. However, they are not capable of detecting new, unfamiliar intrusions, even if they are built as minimum variants of already known attacks [43]. There are many anomaly-based approaches according to Tapiador et al. [44], which can be summarised in the basic modules in the model shown in Figure 5 below.

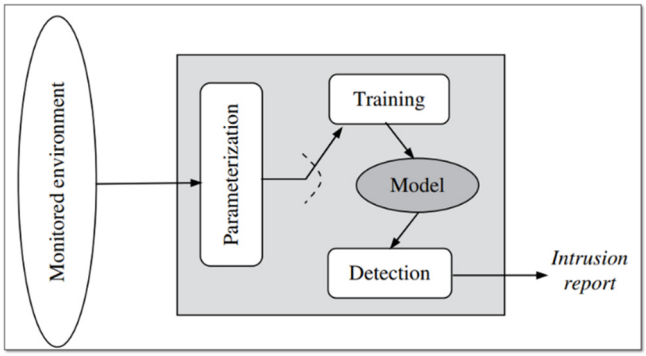

Figure 5. Generic Anomaly model of NIDS [44].

Figure 5 above shows an adaptation of the model represented in a figure of how the interaction works between the various models diagram extracted from Tapiador et al. The three main models indicated are Parameterization, Training Module and the Detection modules as explained below.

I. Parameterization: The target is represented in a pre-established form.
II. Training stage: The normal (or abnormal) behaviour of the system is characterized, and a corresponding model is built.
III. Detection stage: Once the model for the system is available, it is compared with the (parameterized) observed traffic. If the deviation is found to exceed, an alarm will be triggered.

Together with the above NIDs model, there are three approaches that are used to monitor the target and establish its detection rules. These three techniques are Statistical-Based, Knowledge-Based and Machine Learning.

The first one falls under Statistical-Based Techniques whereby the network traffic activity is captured and a profile representing its stochastic behaviour is created. This profile is based on metrics such as the traffic rate, the number of packets for each protocol, the rate of connections, the number of different IP addresses, as described in this particular study by Tapiador et al. [44].

The second technique known as the Knowledge-Based expert system approach is one of the most widely used knowledge-based IDS schemes. However, expert systems can also be classified into other, different categories according to Denning and Neumann [45,46].

These expert systems classify the audit data according to a set of rules, attributes, and classes from the training data. Then, it breaks them down again into a set of classification rules, parameters, or procedures. The audit data are classified accordingly.

The third technique which holds the highest precedence is the highly researched Machine Learning techniques. This method is based on establishing an explicit or implicit model that enables the patterns analysed to be categorized. A singular characteristic of these schemes is the need for labelled data to train the behavioural model, a procedure that places severe demands on resources. Its behavioural models are so advanced with flavours of Bayesian networks (probabilistic relationships among variables), Markov models (stochastic Markov theory), Neural networks (human brain foundations), Fuzzy logic (approximation and uncertainty), Genetic algorithms (evolutionary biology inspired) and Clustering and outlier detection (data grouping) to name the top used [40].

Although anomaly-based detection techniques are not yet mature, they are beginning to appear in commercial and OpenSource products. IDS software tools in this line with Anomaly Techniques include SNORT (www.snort.org (accessed on 15 January 21)) and pfSense [47,48]. Companies that are seeing a growth in pioneering technology include Cisco Intrusion Prevention, McAfee IntruShield Network Intrusion Prevention and Checkpoint IPS-1, which all constitute integral network security solutions [49].

To have a complete anomaly-based technique in its current academic research state has its advantages. It is flexible and adaptable, however, it has a high dependency on the assumption about the behaviour accepted for the system, and of course the high consumption of resource and computing power contributing to financial costs to businesses including SMEs in particular.

Teodoro, G. (2009) survey indicated that Anomaly-based IDS is still in its infancy and as it stands, has a low detection efficiency, especially due to the high false positive rate usually obtained, the low throughput and high cost, mainly due to the high data rates, the absence of appropriate metrics and assessment methodologies and the maturity of analysis of ciphered data [30].

In a paper by Lee, J., et al., (2020) [50], in order to determine if traffic is normal, the classification function in NIDs is important. Here, initially deep learning as a Machine Learning algorithm was applied, however, this method consumed the increase in data management owing to a slow detection in the problems of the NIDs. The proposed research approach then used methods of classifying deep learning based on extracted features, not as a classification but as a pre-processing methodology for feature extraction. A deep sparse autoencoder was used to extract features from unsupervised deep learning models using Random Forest (RF) classification algorithm. Following on, this gave a larger detection dimension on how ML can be further used in the detection of anomaly-based attacks.

6.3.5. Cost Model

In a study by Armenia, S., et al. (2021), the rise in cyber threats has led to SMEs needing to take strategic decisions in their investment in how they can keep their data safe and secure. One framework that was explored in this study was one with international recognition for cybersecurity risk management, Improving Critical Infrastructure Cybersecurity by the US National Institute of Standards and Technology (NIST) [51]. This particular framework whilst providing guidelines and best practices and standards for cybersecurity risk management produces only a static view and still requires self-assessment and the question of highly skilled and equipped staff to manage the process and technology. One suggestion, for SMEs to benefit from having a more suited cost model, is one that is practical and easily adaptable within the business. Armenia's study suggests a system dynamics methodology and tool called SMECRA which stands for SME Cyber Risk Assessment for supporting cybersecurity investment decisions for SMEs through the evaluation of cyber risk and previous investments. The aim of Armenia's study was to propose a methodology that uses SMECRA by using two modules: the Snapshot Survey, and the System Dynamics simulation model (both based on the NIST Cybersecurity Framework).

This framework allows for the evaluation of cyber risks and for the planning of effective investments in SMEs. The study was fixed over a period of two years, in that three SME companies were observed and put through these models. The companies who invested initially in capital towards their cybersecurity wellbeing, showed much better results in resisting cyber-attacks than others that were perhaps lacking in initial defense leading to vulnerabilities. The SME businesses that spent very little monies upfront on cybersecurity were being targeted and suffered much more serious damages.

The model's reference highlighted that on average SMEs spent just under 500 Euros per year on cybersecurity and ended up incurring substantial losses. This amount is not sustainable in getting an SME company to the security level it needs to be within the current climate of increased cyber threats. The model concluded that increasing the investment upfront costs and any damages due to security breaches and time of expertise and staff could reduce the effects of cyber threats. The study performed showed the link between the SME organisation structure using the Snapshot Survey and how strengths and weaknesses of the SME business investments and policies were highlighted using the System Dynamic simulation model. The study focused on the management decisions on where investments were being spent and which departments were given higher priorities in the SME business. The model in this study gave the SME user a chance to simulate any number of highly different cyber scenarios based on various strategic choices and environments before actually committing manpower and financial resources to that area. Introducing SMECRA methodology and tools did have an advantage, as it allowed SMEs to rethink their cyber risk evaluations more accurately, dynamically and be more sustainable at the same time. From this study, these simulations not only displayed the capability and versatility of this model, but they also underscored the importance of prevention and awareness regarding cybersecurity matters, not just for large corporations but also for small and medium enterprises.

In another study of cost analysis by Ahmed, N.N., (2021) investigated the choices SMEs have to make in order to choose the right security solution in place to cater to their business needs. Here, the SMEs were given a survey questionnaire to understand the companies' capabilities in evaluating a cyber threat. This survey was categorised into several selection criteria. One such criterion was Vendor Selection whereby most SMEs would prefer a third part company to perform compliance, physical or enterprise assessment of their network rather than a self-assessment technique according to Ahmed's study. Opting for a multi-vendor approach meant that there was a significant cost reduction in getting a one-stop solution to cover information security issues such as cyber threats. This observation was made in the Middle East with most of the mid-sized companies prefer having a limited budget ranging from USD 1000 to USD 3000 [52]. The next selection criteria were based on finding the right cybersecurity solution, based on known references, peers, and colleagues from the industry as explored in this same study and also the right technology to go with it. Various other sections of the questionnaire went into further detail of devices and NIDS used within these SMEs framework. The study discussed these SMEs going into device and technology contracts to offer support contracts to keep these devices up to date. Ahmed's study cited Mansfield, M., (2017) [53] as revealing that eighty-six percent of SMEs have no efficient means of mitigating cyber hazards even with the right endpoints in place. Endpoint security is an approach to identifying malicious network activity and protecting computer networks from intrusion and malware attacks, including servers, desktops, and mobile devices. Lastly, cloud adoption was a criterion that revealed that only 50% of SMEs were still planning this migration or were not interested in this move to secure their data. Ahmed's study was trying to understand what these SMEs thought of the cloud to secure their data, and most of their SMEs neither agreed nor disagreed. These SMEs seemed content in terms of accepting their cybersecurity strategy as it was. it as well relying on their third-party vendor to perform this job for them keeping all costs low.

In the next section, the examination of the three different NIDs, Cisco and OpenSource, and how they behave towards securing SME data, is evaluated and observed focusing

on the models, algorithms, and cost implications. This will also explain the methodology, findings and analysis of the approach used in the observation.

7. Methodology Applied in This Research

This paper explores the examination of three different NIDs and how they behave towards securing SME data. An evaluation technique was used to observe a commercial NIDs device compared to two OpenSource devices, acting to secure networks originating from the office and home networks.

The commercial device was the "Cisco Intrusion Detection and Prevention Device: Cisco ASA5516x Firepower". This device includes plug-in modules that were bought as part of the license package by the SME for implementation into the security network to protect the customer data. These modules are the Intrusion Protection System (IPS), Advanced Malware Protection (AMP) and URL Filtering Licenses. The two Open-Source devices were SNORT and pfSense that were readily available on OpenSource for free. To add to this scenario, the research study was conducted during the global pandemic of COVID-19 during 2020 which reflects the rise of cyber-attacks on technology.

According to Kothari [54] "research" refers to the systematic method consisting of identifying the problem and leading to a collection of relevant facts and data in order to formulate certain conclusions towards the question that is explored in the study. This involves the application-specific methods to gather the information, and in the observation method, would involve the investigator towards the concerned problem. In this particular study, there is the observation of the frequency with which certain identified variables are occurring and whether they occur in relation to associated external variables. This is relevant to this study where the observation is unique and does not involve large samples and is only on a particular case. The conclusions that emerged will enable the researcher to relate the findings towards the broader objectives of the research question which is to explore the wider implications of the cyber threats on networks. This observation empirical methodology was applied to the three empirical cases adopted in this study, each having its unique locational scenario. All three devices see network traffic coming into the network from a private and public display of data from SMEs and their employees working from the office and from the home environment.

7.1. Three Scenarios Explored in This Study

In order to understand the scale of the detection systems (IDPS) as a whole, there were three scenarios that were studied. All three were studied through empirical observations focusing on the models and algorithms described in the previous sections.

I. Evaluation of the hybrid IDS-Cisco Firepower in a live office network
II. Evaluation of the pfSense as a jump Server in a hybrid office and home network
III. Evaluation of SNORT in a home network

7.2. Evaluation of the Hybrid IDS-Cisco Firepower in a Live Office Network

In this section, an evaluation of the Cisco ASA5516-X Firepower inclusive of the Intrusion Protection System (IPS), Advanced Malware Protection (AMP) and URL Filtering Licenses was conducted. The privilege of getting live data from observing how traffic flowed in the data centre of the SME showcased in this study gave visibility of live traffic information from good and bad patterns. This SME provides IT support to its customers and relies on GDPR compliant devices of IDPS, in order to maintain the integrity of its data for protection and safety from attacks. The next subsection explains the experiment conducted and observed followed by the findings and analyse of this first evaluation.

7.2.1. Case Study of Cisco ASA5516-X Firepower

The Cisco product used in this live environment markets itself as a leader in threat-focused next-generation security services. The Cisco ASA5516-X with Firepower Services is centrally managed by the Cisco Firepower Management Centre, which provides security

teams with comprehensive visibility information and control over activity within the network [55,56]. The engineering team of the SME has direct access to this Cisco security team together with any up-to-date patches and security features available.

According to Cisco, their Firepower System can help in monitoring the network for traffic that could affect the availability, integrity, and confidentiality of a host and its data. By placing managed devices on key network segments, the device can examine the packets that traverse the network for malicious activity. The system has several mechanisms it uses to look for the broad range of exploits that malicious actors have developed.

The system uses Intrusion Prevention System (IPS) to monitor the event and cut off any connections to the attacks. This information is a record of the date, time, the type of exploit, and contextual information about the source of the attack and its target. Managed devices transmit their events to the Firepower Management Centre (FMC) where data can be viewed, and the aggregated data can be gained for a greater understanding of the attacks against the network [57].

The Cisco Firepower records these intrusion data as Impacts to the networks. The impact level indicates the correlation between intrusion data, network discovery data, and vulnerability information. It ranges from Impact Level 0 to Impact Level 4. The Firepower is also able to identify the IP addresses used by the receiving host involved in the intrusion event called Destination IP (Syslog: DstIP). The Firepower also provides information of Classifications where the rule is able to generate where the event belongs.

The Firepower plays two important roles, one as the IDS and the other as the IPS thus completing a full IDPS integrated system. Through the Security Info Event Management (SIEM), the Firepower is able to produce data and alerts when intrusion is detected, send alarms, and prevent the intrusion.

In the next section that follows, the Firepower is evaluated in this live environment and its results analysed. This environment was the operating system in the SME which is the industry party in this study. The results reflect empirical observation and analysis of data of the network. The results will be examined as to what is being captured and subsequently the method of approach used from a scientific model and how this is applied to a real-life business of IT management.

7.2.2. Analysis and Findings

The Firepower evaluation was done on the Cisco Intrusion Detection and Prevention Device: Cisco ASA5516X Firepower inclusive of the IPS, AMP and URL Licenses. This device is manufactured by Cisco and is a hybrid model that uses the hybrid model of statistical analysis combined with features of the machine learning algorithm of behavioural analysis. The Cisco IPS network-based intrusion prevention system (NIPS) uses signatures to detect network-based attacks [55,56].

Data from the Firepower were extracted and were analysed for the month of March, April, and May 2020. The results captured showed traffic and intrusion events over time from 20 April to 18 May 2020. Within the results, it was noticeable that spikes were observed through mid to end of April when the UK was preparing to go into lockdown. These spikes were intrusion events occurring around those dates. The Firepower was able to detect these events and log an audit trail and give an output in the form of a graph and alert.

The Firepower was also able to share details of the Classifications and Priority of these Intrusion Event Details during this period of each event. It showed the type of events against classification, priority, and the number of times these events took place. Classifications such as “Web Application Attack”, “A Network Trojan was Detected”, “Attempted Information Leak” and “Attempted User Privilege Gain” were amongst those that were identified by the Firepower. Priorities such as “high” and “medium” were given against these classifications and the number of times these events occurred were counted.

Classifications such as "Web Application Attack" occurred 171 times via an SQL injection attempt. The Firepower gave this a high priority and regarded this as high importance. Events identified ranged from SQL injection, malware detection and console attempts.

Through a selection of workflows and drilldown events, the Firepower was able to also detect source countries such as China making multiple intrusions and their source IPs. The Firepower was also able to identify the Destination IP and the country being the UK.

The Firepower was able to show detection from country China and its malicious actors trying to penetrate the network and the device IDS dropping this intrusion. The Firepower was able to show detection on when the device had dropped this connection from China as it recognised it to be a harmful attempt into the network and stopped it before any malice was attempted. In particular, categories of files used to try to penetrate the network from Firepower were the likes of multimedia, pdf files, office documents and executables.

The Firepower was also able to show the intrusion by Geolocation and by where the hacking originated from as seen from Figure 6 below.

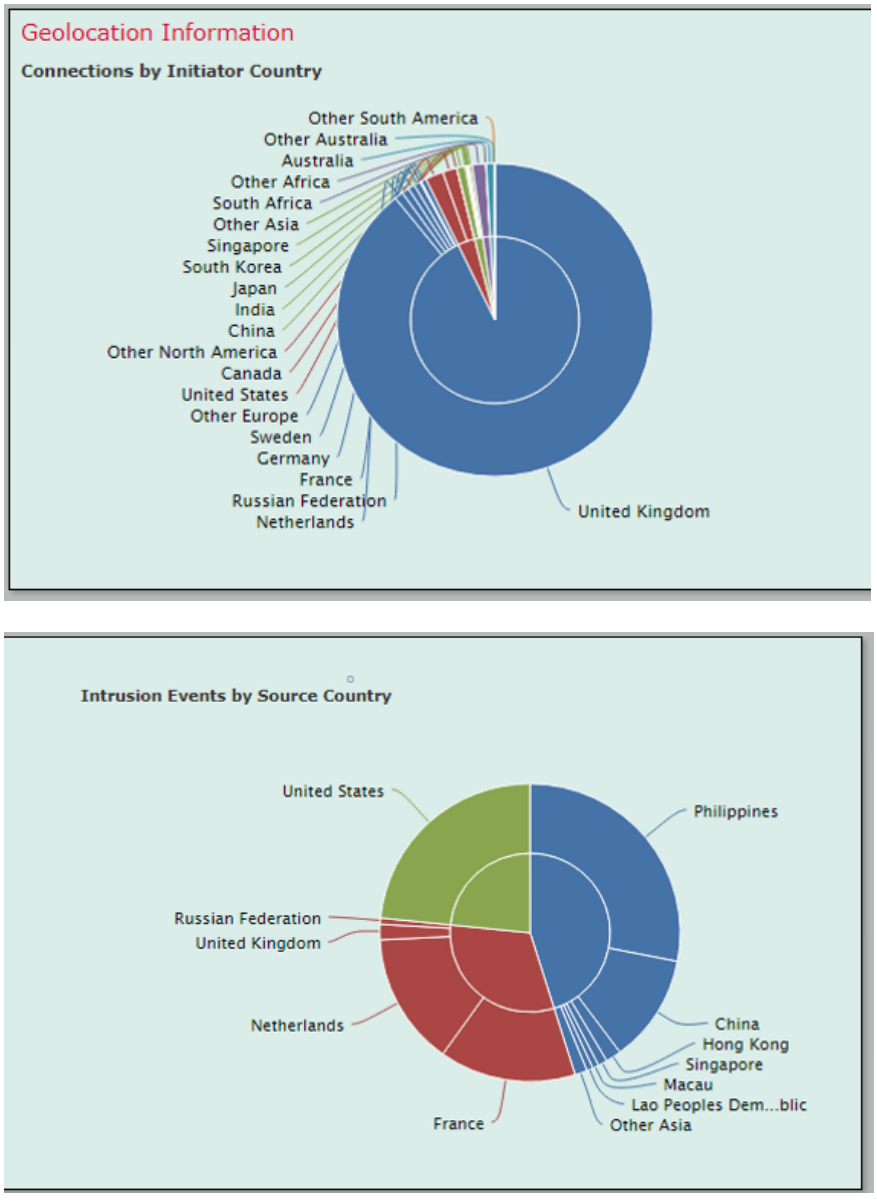

Figure 6. Geolocation Information extracted from Firepower.

From the pie charts above, a list of all the countries trying their hacking techniques can be seen in the case of the UK.

The Firepower was also able to extract information such as the Top File Types Received via the network from Figure 7 below.

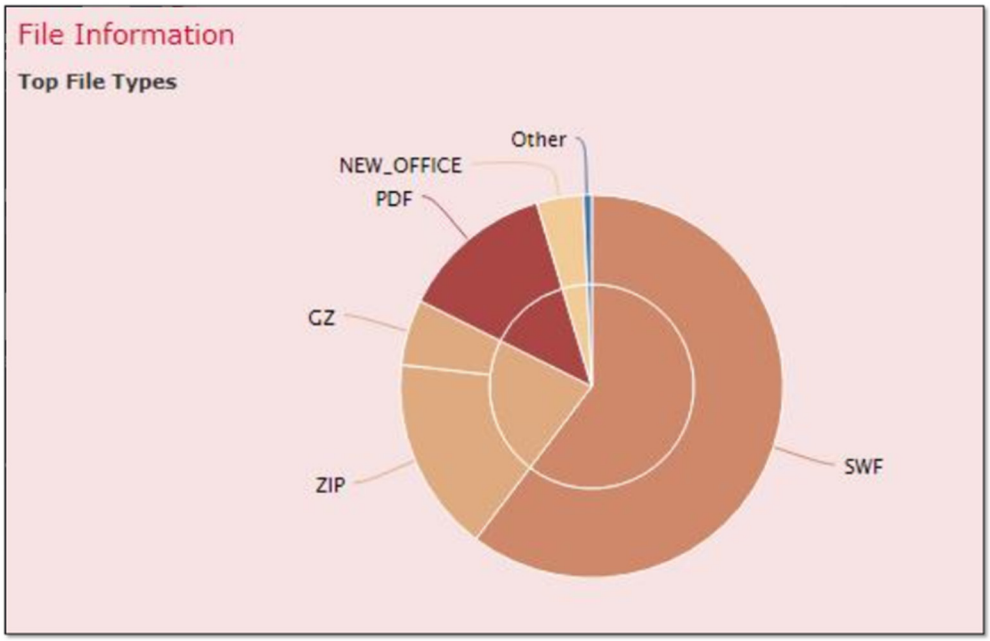

Figure 7. Top File Types extracted from Firepower.

It can be seen from the chart in Figure 7 above, that files with extensions of .SWF, .ZIP and .PDF were the files that were infected and caused harm and were detected and securely quarantined and scanned before being released.

The Firepower also had the reports to extract Top File Names that tried to penetrate the network during these months as shown in Figure 8 below.

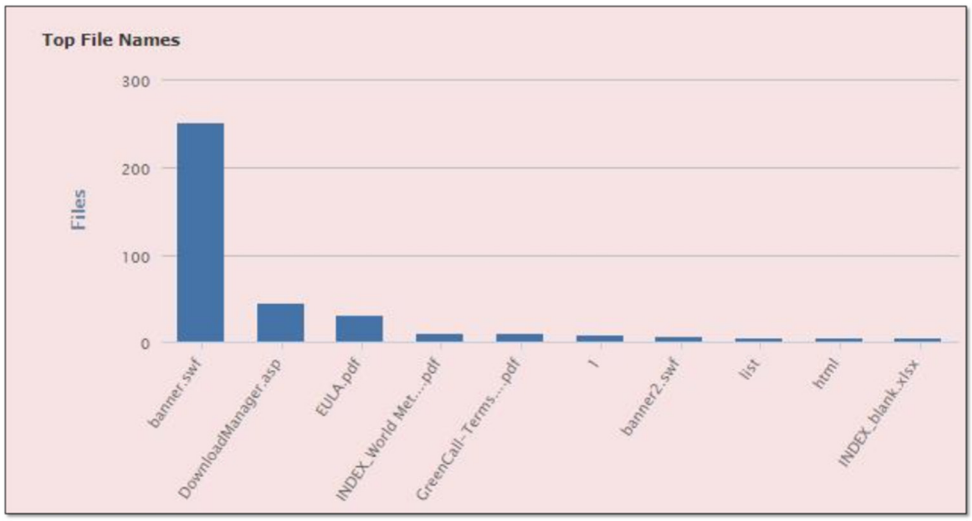

Figure 8. Top File Names extracted from Firepower.

As mentioned previously, Impact was an important ML classification in terms of the detection period and the preventative measure that took place during these months. The following chart in Figure 9 below showed high Impact as zero (0), and medium Impact indicated as a one (1).

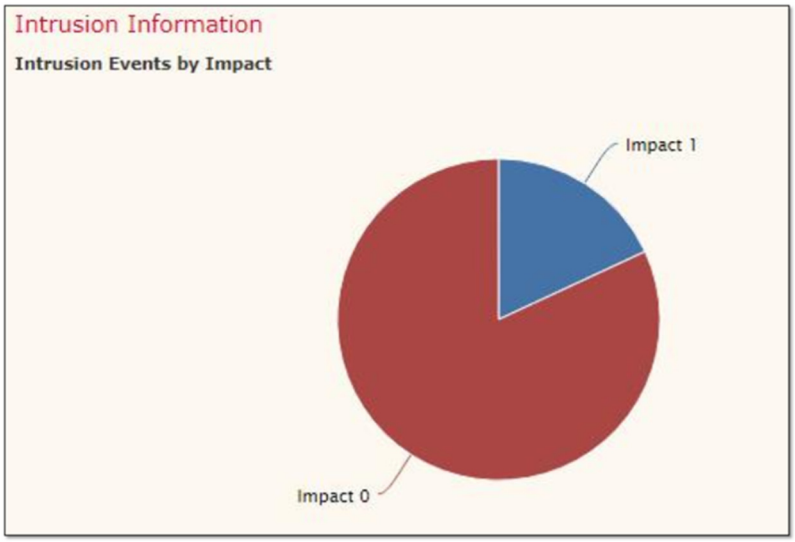

Figure 9. Intrusion Event by Impact extracted from Firepower.

These impacts shown in Figure 9 indicate the value of the potential severity of an attack. Figure 10 below was particularly interesting because it identified all the application protocol information and the types of Traffic by risk and application.

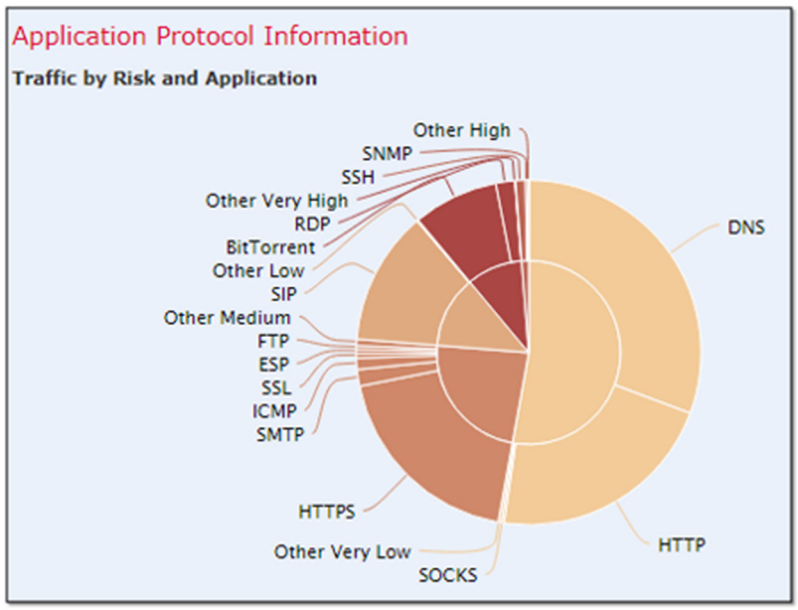

Figure 10. Application Protocol Information: Traffic by Risk and Application extracted from Firepower.

Figure 10 above shows HTTP, RDS and DNS are amongst the top traffic going through the network that contributes to the risk applied on the network. Monitoring these protocols and their behaviour and what they connect to will allow the detection to be positive and react with the right prevention mechanism in place.

Findings further showed that during the setup process of the Firepower, the Cisco IPS used the signature-based approach for detection and prevention, as it was less of a strain on the computing power of the device and network. It also used less memory and impacted the CPU performance less on the IPS device permitting more signatures to be active as suggested by a blog on Cisco performance online based on its usage as defined in the experiment [55].

In accordance with Cisco, in order for the SME to move to a complete anomaly-based approach would mean that extra plug-in modules would have to be purchased to have

more ML featured available to test even further. The costs would reflect a rather high amount per month as Cisco relied on a subscription-based model for its customers to use the ML features to its full potential. The SME in this experiment did not buy into the extra modules due to their own monthly contract costs with the customers not reflecting the uses of the full potential of ML features. The experiment only showed ML features that were already pre-prescribed and basic in the features and levels of intelligence supplied. Another cost implication would mean the increase in ML features having a direct impact on the cost of CPU performance which was not feasible due to the level of the cost incurred for the SME in question without having to cross charge this back to the SME customers. From this evaluation, it was found that there are devices and software applications that can be combined to raise the detection and alert so that prevention can act faster and damage control can be managed. In order to reduce the main Cisco cost of using the full potential of ML features, SMEs businesses have to seek alternative protection to addresses advance anomaly-based approach ML to help benefit their NIDs from zero-day attacks by implementing the following into their network. Following are the three layers of ML techniques applied by SMEs from a cost perspective.

- Anti-virus products that are effective for detecting malware that is active on the network that uses ML techniques.
- Port access that is filtered efficiently by traditional firewalls that require manual intervention by engineering expertise within the SME.
- Application firewalls control access to applications wall products by filtering input, output, and system service calls locally and over the network again manual process by engineering intervention.

Cisco ASA with Firepower services brings distinctive, threat-focused, security services that provide comprehensive protection from known and advanced threats, including protection against targeted and persistent malware attacks. During the evaluation, there were modules of the Firepower that could only be triggered through a subscription model. The devices are very powerful but costly to run as the features increase and are switched on. Nonetheless, with its basic IDPS model in place, the device was able to provide the SME with statistics on a monthly basis to help protect the SME customer's environment in this ever-changing cyberspace and carry on protecting their data.

7.3. Evaluation of SNORT (Open Access)

7.3.1. Case Study of SNORT

The SNORT intrusion detection was conducted as a comparative to the evaluation of the Cisco device in the above section. SNORT is regarded by its creator Martin Roesch, as a Lightweight Network Intrusion Detection System [58]. According to M. Roesch,

> "Commercial NIDS such as Cisco have many differences, but Information Systems departments must face the commonalities that they share such as significant system footprint, complex deployment, and high monetary cost. Snort was designed to address these issues."

SNORT is regarded as a clever way of manipulating its rules to work in the environment of your choice. Its codes and rules rely on people who are able to change the codes and rules to fit the purpose of their experiments to detect cyber threats. Due to the nature of where it is available, this allows the rules and codes to be freely used by anyone. In some cases, these codes and rules are adopted by larger technology vendors and become embedded into their own existing devices as later observed in the comparative tables [51]. According to Roesch, SNORT can also be deployed rapidly to fill potential gaps in a network's security coverage, for example when a new attack happens, and commercial security vendors are slow to release new attack recognition signatures. The cost of SNORT is also very low compared to those of Cisco and other commercial vendors. It is free to download however comes with minimal support costings on a monthly basis to

subscribe to the community of SNORT followers in order to maintain UpToDate software when released.

SNORT is a specific type of packet sniffer referred to as "libpcap-based [PCAP94] packet sniffer and logger" and can be used as a lightweight network intrusion detection system (NIDS). It features rules-based logging to perform content pattern matching. This allows the device to detect a variety of attacks and probes. SNORT is famous for its performance, simplicity, and flexibility.

Figure 11 below shows a simple SNORT rule:

```
log tcp any any -> 10.1.1.0/24 79
```

Figure 11. Simple SNORT rule extracted from SNORT website [58].

This rule above records all traffic inbound for example an identified port "79(finger)" going to the "10.1.1 class C network address space" as explained by Roesch [58]. SNORT uses a Bayer–Moore algorithm to perform its pattern matching, regarded as one of the best algorithms available for that task. It achieves its greatest efficiency in cases where the pattern to match consists of non-repeating sets of unique bytes as described by Roesch.

The application of SNORT was downloaded and run, in a live home environment. The application was run during the month of June 2020 which coincided with the COVID-19 lockdown in the UK. As such, the constraint of COVID-19 had to be considered for the conduct of this observation in the domestic setting.

The environment was a domestic setting in a household with a Virgin Media Router serving the purpose of the firewall to several IoT devices connected to the router via the internet. SNORT was downloaded and ran as per the instructions on the SNORT website [58]. The most recent version of the packet sniffer was downloaded. SNORT took a three-step process to download and run the executable. Step1 and Step 2 were the "Get Started" sections. Step 1 was to download the executable so that the executable could run in a Windows Environment.

Registration of an account was part of Step 2, so that the rules available could be used which had more options if the user were not registered. This is a method in which SNORT uses to gather information from those using their software to share any upgrades and new rules shared amongst its community. Step 3 was setting up the Rules and the type of Rules that were needed to perform this detection.

Signing into the account gave visibility of not only the Community Rules, but also the Registered Rules. Subscription could have been a further option however this would have had to be paid upfront for further subscription rules. This would have costed money and at this stage of the experiment, only the basic rules were required for the detection run.

Once the package was downloaded, unpackaging and running the software was required on Windows Application. Tips were shared through the guidance of YouTuber Steve Gantz on his channel and show, on how to install SNORT 2.9.8 on Windows [59]. According to Gantz's instructions, the application WinCap and Wireshark had to also be downloaded to assist in the running and logging of this packet sniffer. The most important guidance also was the changing of the SNORT rules so that SNORT was able to monitor the home network and log any attacks that occurred on the devices that were managed in the same household. Figure 12 below shows where SNORT was stored in the C drive and how it was run.

As seen in the install directory folder structure above in Figure 12, there were two main rule folders:

I. rules
II. preproc_rules

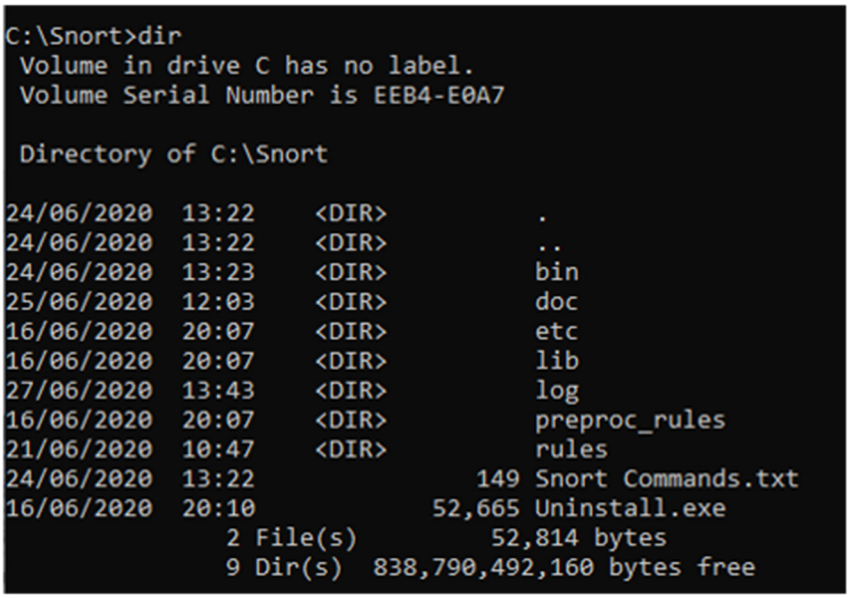

Figure 12. Location of SNORT folders extracted from SNORT website [44].

The network detection at the domestic house location was able to operate due to the combination of both rules. An independent file and default working structure, "snort.conf" file, was downloaded and provided the main configuration file to run SNORT. This file contained all the links to all the rules in the SNORT directory. There were several steps that had to follow to make sure SNORT understood "where it was" and "what it was trying to detect". Several steps had to be configured in order for SNORT to work, and this included the home IP address. The configuration files were quite comprehensive and anyone who knows and learns the SNORT rules is able to adjust the rules and code even further. Once the rules were established on what was required, the next step was to run the configuration file and the results were then stored in the log files. Wireshark was downloaded to analyse and evaluate the logs.

7.3.2. Analysis and Findings

In the observation, a third-party network scanning application tool called IP scanner was used to identify the IoT devices on the home network as shown in Figure 13 below.

Figure 13 above shows a breakdown of the IoT devices connected and their manufacturer plus the MAC address of the device. Additionally used was Wireshark, also an OpenSource Software released under the GNU General Public License. The GNU is a widely used free software license that allows users the freedom to run, study, share, and modify the software.

Figure 14 below shows an extract of the sample data analysed from the SNORT log files using Wireshark, a more advanced tool for IP scanners.

The results merely show the types of regular traffic that could be seen if connected to the internet in general from home whilst working, playing games, and watching YouTube. Figure 15 below shows the protocols that were captured during this time period, and this shows the variations and counts of these protocols over this period of SNORT capturing this information.

Status	Name	IP	Manufacturer	MAC address
	routerlogin.net	192.168.0.1	NETGEAR	50:6A:03:07:47:EB
	192.168.0.2	192.168.0.2	Zentri Pty Ltd	4C:55:CC:1C:47:13
	192.168.0.3	192.168.0.3	NETGEAR	28:C6:8E:78:2C:48
	192.168.0.4	192.168.0.4	ARRIS Group, Inc.	50:95:51:C1:1D:8E
	HP679A1A	192.168.0.5	Hewlett Packard	70:5A:0F:67:9A:1B
	192.168.0.6	192.168.0.6		A8:DB:03:4E:64:C0
	192.168.0.7	192.168.0.7	OnePlus Technology (Shenzhen)...	94:65:2D:C9:61:2B
	192.168.0.8	192.168.0.8	OnePlus Technology (Shenzhen)...	94:65:2D:D1:B0:BB
	WR302432ADE765	192.168.0.9	Intel Corporate	30:24:32:AD:E7:65
	192.168.0.10	192.168.0.10	Intel Corporate	5C:C5:D4:6D:CB:5D
	DESKTOP-FLHQV...	192.168.0.11	Microsoft	B4:AE:2B:C7:D1:E6
	192.168.0.13	192.168.0.13	AzureWave Technology Inc.	6C:AD:F8:B2:F9:69
	192.168.0.14	192.168.0.14	Apple, Inc.	5C:AD:CF:EA:D6:A8
	192.168.0.17	192.168.0.17	AzureWave Technology Inc.	5C:96:56:20:A6:37
	DESKTOP-2IQJ1UU	192.168.0.18	Liteon Technology Corporation	D0:DF:9A:1A:BF:A0

Figure 13. IoT Devices connected to the home network using IP scanner.

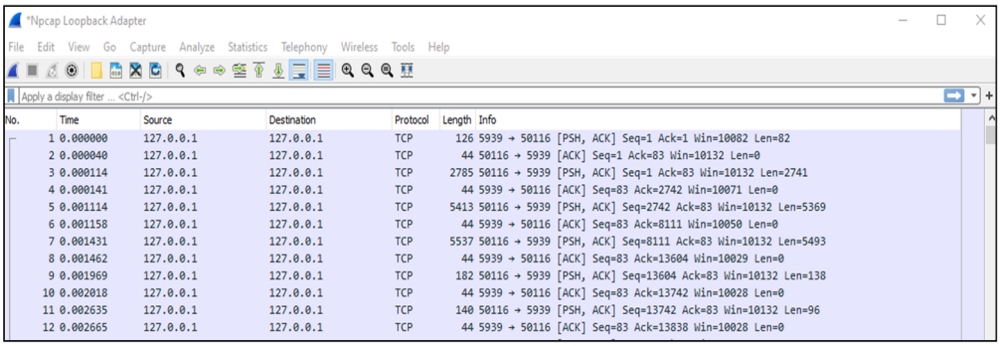

Figure 14. SNORT log file in Wireshark.

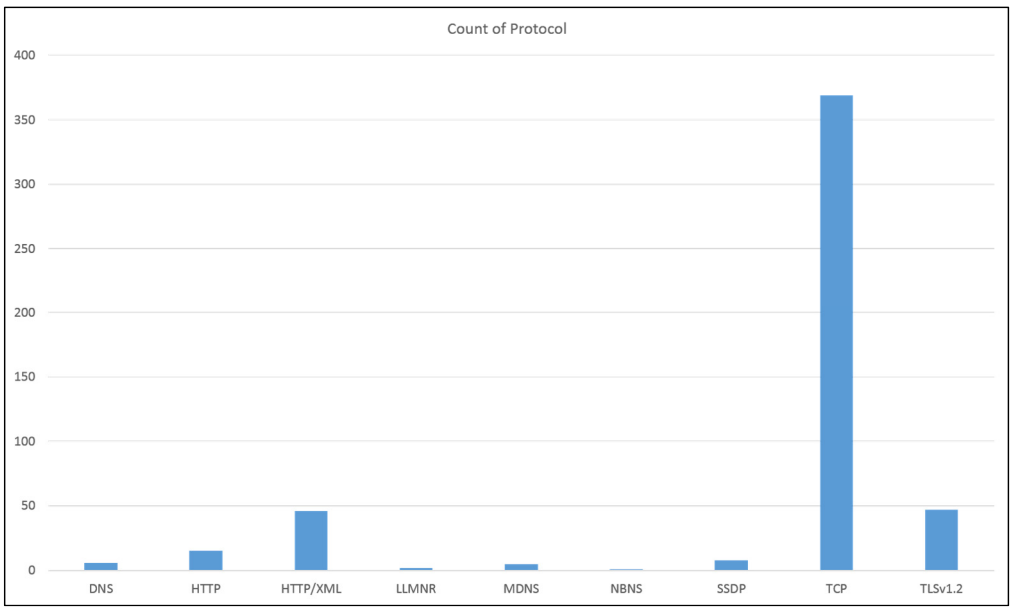

Figure 15. Protocol versus the Count Number of Times Protocol was Detected by SNORT.

Figure 15 above shows evidence of Transmission Control Protocol (TCP) which is IP traffic which is the normal behaviour for when we connect to the internet and the number of times it was detected noting the count of the protocol. It was good to see that the results captured TLSv1.2 which is the Transport Layer Security as this is vital in securing the network traffic and how users browse the internet. Amongst other protocols that were captured, the HTTP/XML was also an important protocol to identify, as this shows the detection of any XML coding that could potentially arrive at the user's session and could potentially cause threats to the system. XML documents are very frequently used in the transmission of viruses through the internet. This shows that SNORT was able to identify when users are accessing normal pages or xml coding database backend pages.

The findings show that it was easy enough to install and run SNORT. The rules were easy enough to change once the process was clear on how to do this from various sources on the internet. The training available to SNORT is by self-teaching however did require someone who was highly trained to perform more complex network detection. SNORT was free to download and use, and its costs were minimal. The adaptation and use of other software to complement SNORT to analyse the data and the findings took some comprehension from experts in the field. Wireshark was used to assist in the completeness of this observation. It was clear that whilst this observation was running, there were no threats to the home network and that users were operating in a secure and safe environment connected to their office network. The ideal scenario moving forward would be to see how this behaviour changes in an office and commercial setting with more devices connected compared to the home network, and more exposure to the internet worldwide in a direct link within the office environment. The home scenario was subjected to a family-run network with certain rules applied on the Virgin Media router that had links to the office network via VPN connections. Due to the COVID-19 lockdown, the observation and experiment also involved and exposed other IoTs within the household generating traffic in sudden spikes in threats happening due to the shift in working from home. Certain rules were changed on the Virgin Media router to reflect the safety of browsing, how browsing was done and the times in which browsing was allowed.

7.4. Evaluation of PfSense (Open Access)

7.4.1. Case Study of PfSense

In 2016, pfSense was introduced into the SME business as part of an ongoing test of various NIDs that could complement other Cisco devices in the SME data centre. Here, pfSense, like SNORT, is an OpenSource set of rules that is free on the internet. At the time back in 2016, the engineering expertise was present therefore the setup and use of pfSense to detect and protect the network in a commercial environment were feasible. Due to the introduction of GDPR and Data Protection, the SME switched to Cisco standard devices in order to comply hence overlooking the somewhat capability of what pfSense could have brought to the table. Further, pfSense is now used in the SME business as a Jump Server for any engineering tasks that are being conducted via its outsourcing partner supplier.

The product pfSense [48] is a customized Free Berkeley Software Distribution (FreeBSD), primarily oriented to be used as a firewall and router. Again, pfSense is an IDS package freely available on OpenSource under the same GNU License as SNORT. However, pfSense mainly focuses on full PC installations rather than the network level. The pfSense is currently a viable replacement for commercial firewalling and routing packages, including many features found on commercial products such as Cisco Pix, SonicWall and WatchGuard. The list of features, among others, include the following such as firewall, routing, QoS differentiation, NAT, Redundancy, Load Balancing, VPN, Report and Monitoring, Real-Time information, and a Captive Portal. It is capable of managing high throughput scenarios (over 500 Mbps), as long as high-end server-class hardware is provided. Further, pfSense uses a single XML file, called config.xml, which stores the configuration of all services available. The code responsible for the operation of the distinct pfSense services is essentially written in PHP, which makes it easy to extend the current code base, improving

existing features or adding new ones. The following will go on to explain how pfSense is currently being used in the SME environment and how it is acting as an IDS for a Jump Server in both a hybrid setting of the home and office environment.

This observation took place in the SME business data centre in May 2020, also coinciding with the COVID-19 lockdown. Earlier in December 2019, the SME business noticed a lot of attacks from other countries including China and eastern European countries, the US, and Africa, and took a decision that pfSense would not be opened to countries outside of UK. The only exception was the engineers who worked abroad in India with their specific IP address working from home, who are part of the expert support for the SME in their professional capacity. Following the observation, an extract of the log files was taken and observed as part of this study. The extracted log files were then exported into Excel for further analysis.

7.4.2. Analysis and Findings

In the observation, it was found that pfSense was able to give an extract to show the activities on the risk of application and protocols. Figure 16 below shows the variations in protocols observed by pfSense.

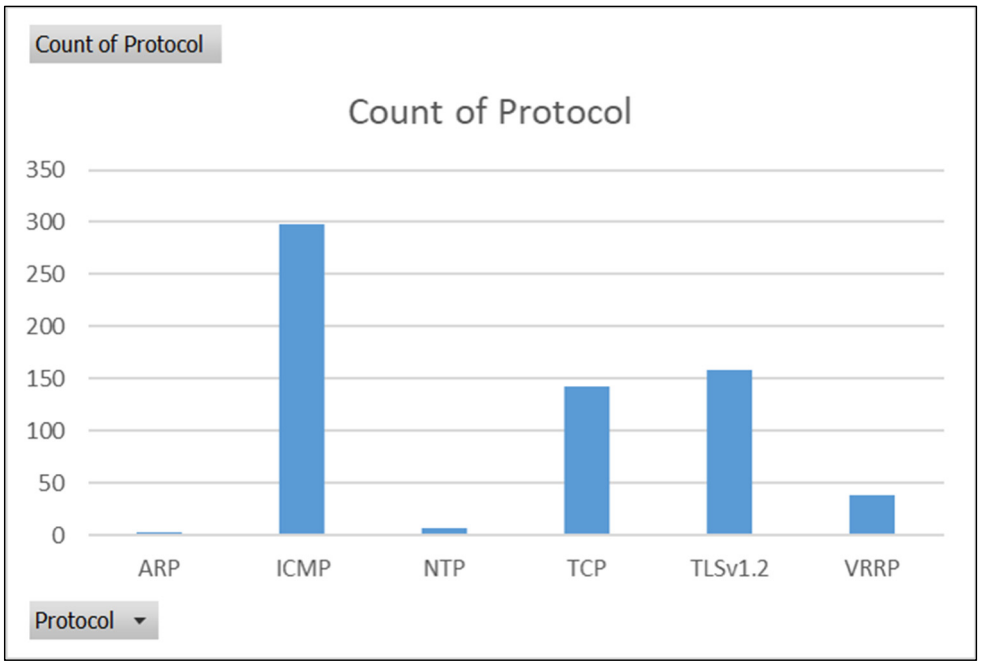

Figure 16. Protocols from pfSense extracted from pfSense.

Figure 16 above shows a difference in protocols compared to the other devices observed and the number of times this protocol was detected. In particular, Address Resolution Protocol (ARP) in identifying MAC addresses. Internet Control Message Protocol (ICMP) where the internet layer protocol is used by network devices to diagnose network communication issues. ICMP is mainly used to determine whether or not data are reaching their intended destination in a timely manner. Other matters that were familiar were TCP and TLSv1.2. VRRP and NTP refer to IP protocols and how the network is routed and timed.

The second set of data shown shows the number of counts of different destinations that try to introduce themselves to the network via pfSense. It is through this detection that it was clear who was trying to access or tap into the SME business network. Figure 17 below shows the Destination Counts via pfSense Detection.

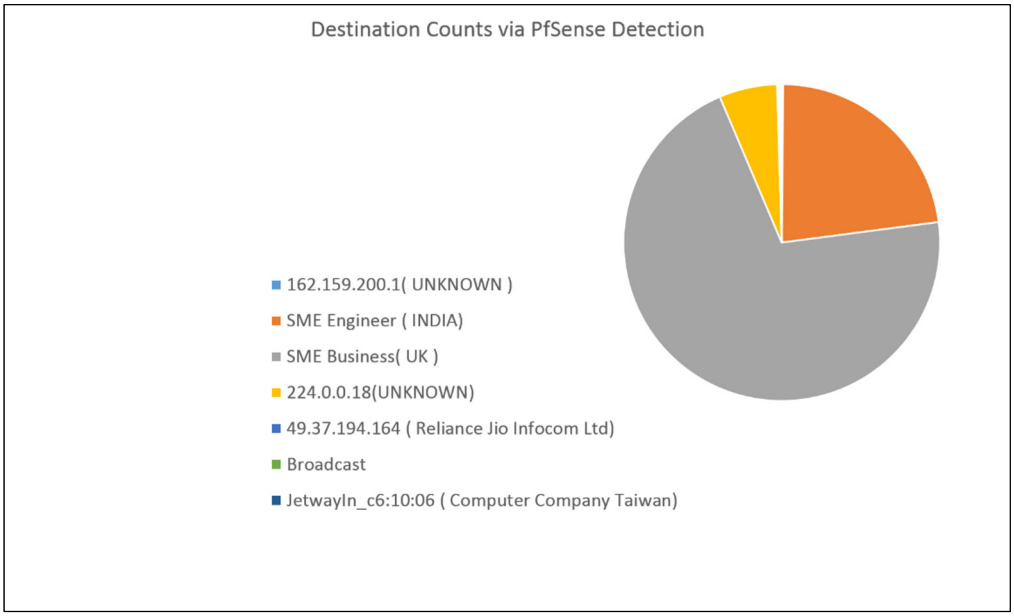

Figure 17. Destination Counts via pfSense Detection extracted from pfSense.

Figure 17 above shows that the majority of the counts detected was from the engineering team in India using the Jump Server to gain access to the SME business data centre in the UK and vice versa. However, in this extract, it can be seen that some anomalies of others also trying to gain access into the data centre in the UK. These were coming from Taiwan and China. Some attacks are very smart and therefore pfSense is not able to identify its source. This shows that free OpenSource access tools can detect very low levels of network traffic and be able to prevent any anomalies from happening. The use of pfSense within this observation proves that these layers of filters enable these applications to work collectively to detect any patterns that are unpredictable using internal ML techniques very often not known to the end-user such as this SME. In order to take advantage of the varying levels of ML uses within these products requires yet again a level of knowledge and technical expertise plus a financial commitment in order to open these layers of code up to see what is happening within the algorithms.

This concludes the three evaluations based on the experimentation's setup in both the office and home environments and discusses the concepts of costs versus ML knowledge in order to predict and capture zero-day attacks.

The next section explains the general use of how Security Incidents and Events Management systems take a prominent stage in SMEs to manage these incidents and activities. Methods of reporting back into the business are explored in order for these SMEs to make informed choices on how to protect SME data and the SME business from both angles of office and home working.

7.5. Security Incidents and Events Management Systems (SIEMs)

SMEs use various different software to manage their Security Information and Event Management Systems (SIEM). These software's are very complex systems and uses a large number of functions with different behaviours as shown in a study by Sönmez, F.Ö. and Günel, B., 2018 [60]. As cited in this same study, visualization is a common way of data presentation in these systems along with other data presentations such as reporting, alerting, text messaging. As seen from the analysis and findings of the three scenarios explained above, all IDPS devices were run from their own SIEM software. This allowed the research to show a graphical representation of the results. This then allowed the research to reach a conclusive evaluation of the information for these tools. SIEM systems according to the same study and through the experiment conducted in this paper, showed that purchasing the most useful SIEM system with the IDPS device for an organization

produced a good translation of numbers. The SME in this study used various SIEMs such a Solarwinds, Cisco, Tripwire, Wireshark and Splunk to name a few. The next section brings together the three IDPS and how they compare against each other using information that was extracted from SIEMs.

7.6. Comparison: Observation of Cisco ASA 5516-X FirePower, SNORT and pfSense

The above sections gave the outcome of the observations based on the various case study applied. All three devices that were evaluated and used in the observation were recorded and their differences were captured. It was clear from the analysis and findings that there were significant differences and similarities between the three devices. All three experiments were conducted in an environment where live data were used and internet bandwidth utilised. The office experiment used the live data centre as its collection of data via its firewall. One example of variables that were controlled was its Geo-Location, where these attacks were coming from, and other variables within the IDPS settings. The home scenario was also the same in accordance with the router settings and configurations set up by Virgin Media. This also had a dependency on how the IDPS was configured within the home network. All three experiments were streaming random unknown attacks from cyberspace. The comparative results can be dissected as explained in the next paragraph under Table 1 below.

Table 1. NIDS Device comparison.

NIDs Devices	Cisco-FirePower	SNORT	pfSense
Experiment	Office—Live Data Center	Home	Hybrid—Home and Office
Financial Costs	Software and Hardware: £10K–£15K Capital, £5K over a period of 3 year subscription model for support and updates. Engineering Staff Cost: £30K–£40K salary per annum based on experience	Software and Hardware: Free to download. Donation to SNORT community. Hardware: High spec PC; £1K–£2K Engineering Staff Cost: £30K–£40K salary per annum based on experience	Software and Hardware: Free to download. Donation to SNORT community. Hardware: High spec PC; £1K–£2K Investment of Hardware to Govern the power of the Opensource Engineering Staff Cost: £30K–£40K salary per annum based on experience
Rules	Rules cannot be changed, its embedded into the Firepower and lined back to Cisco as the control mechanism. Cisco also have bought certain ML aspects of SNORT and pfSense rules and embedded them into their algorithms.	Rules can be changed and integrated very easily. Rules are simple to write; Rule based Content Pattern Matching however requires engineering knowledge susceptible to human error.	Rules can be changed and integrated very easily. Rules are simple to write; Rule based Content Pattern Matching however requires engineering knowledge susceptible to human error.
Types of IDS	Signature, Anomaly ML features on subscription	Signature, Anamoly, Machine Learning	Signature, Anamoly, Machine Learning

Table 1 below shows the varying NIDs device and the differences between them. From this, the table shows the outcome on a comparative basis. There were three elements that were compared, and this included the financial costs associated with implementing the NIDs, the type of rules that were used and the different types of IDS methods followed plus the hardware to run the software.

Table 1 above shows that there is a distinct difference in cost and flexibility of the rules. The Cisco Firepower is very high in capital cost and its devices and monthly support are in the range of GBP 10,000–15,000 as explained by the SME business taking part. Monthly payments have had to be cross charged as part of the service back to its customers who utilize this server of the IDS. SNORT and pfSense on the other hand are free, however, the knowledge and the expertise of engineers and their knowledge are a separate investment

to be able to run confidently these rules in a commercial GDPR compliant environment. Without this expertise, the commercial sector would not be aware of how to manage this IDS moving forward.

From this observation, it also came to light that Cisco as a technology vendor and market leader has already absorbed parts of SNORT and pfSense rules. This is largely due to their resourcing expertise. SNORT has been used to fill holes in commercial vendor's network-based intrusion detection tools, such as this Cisco FirePower. When a new attack makes its debut in the hacker community and signature updates are slow to come from the vendor, SNORT is then used to characterize the new attack by running it locally on a test network and determining its signature.

The findings of this work suggest that it is easier for Cisco engineers to use those rules from SNORT and pfSense and embed them into the listing above than to release new codes of their own. Due to the fact that SNORT is a packet sniffer, this allows its machine learning algorithms to fit nicely within the Cisco framework.

Following on from the observation and the findings above, it is now appropriate to bring the discussion to a conclusion in the next section.

8. Conclusions

The realities of threats have evolved into both technologies as well as wider policies towards managing threats. Protection of data, as seen in this paper, is the reason why IDPS systems have come into force. The ever-changing demographics of the internet invite hackers and malicious actors who are getting cleverer and using technology to try and bypass the good systems the world is trying to put in place to protect its data. GDPR and cybersecurity models are platforms in which compliant standards are put in place for countries to implement and SME businesses to feel safe in an environment that is structured and has a process. However, this can only be met if the right people through education and communication put these processes and procedures in place. As for the devices in the market, hybrid solutions and affordable devices need to be at a balance on how our data are managed and kept safe within the SME market for those in the safety of the office environment and a hybrid solution working its way into the home environment as a result of the COVID-19 pandemic shift of working.

The study showed the comparisons between Cisco, SNORT and pfSense. There were three different IDS, and their features were compared. It was concluded that whilst SNORT and pfSense were free to use from the OpenSource Market, it required a certain level of expertise to implement and embed the rules into an SME business solution. It was also noted that Cisco, due to the company's engineering expertise and its position as a market leader in the industry, was able to embed these free rules and use them to their advantage. For an SME business, this outcome, although bearing an upfront cost to the business, shows a more feasible and working method towards showing compliance and GDPR in its infrastructure through the usage of Cisco IDS. Further, the models and algorithms used are automatically updated through a Cisco device provided a subscription model is taken. The study showed that Vendor Suppliers have a better model in place to provide their SME customers with a balance of highly skilled expertise including highly comprehensive technology in order to find the balance of securing their data. This balance is shown in the monthly costs to the SME customers and the infrastructure of how these devices get updated and keep on securing clients' data.

Machine learning approaches such as Signature-based models can only detect attacks that are known whereas Anomaly-based systems are able to detect unknown attacks. Anomaly-based IDS makes it possible to detect attacks whose signatures are not included in rule files. Unfortunately, due to the maturity of Anomaly-based IDS, the costs are still very high to run and it requires computing power that is unrealistic in our developing environment. Anomaly-based IDS, whilst still in its infancy, also requires a deeper analysis and future study. Alternatively, proposals that are feasible and affordable need to be addressed in the near future in the field of IDS with confidence.

Therefore, it is crucial for SMEs to also understand how Machine Learning plays an important role in the detection of zero-day attacks. However, this does come with a cost. Understanding this cost is important for SMEs to be aware and thus understand the need to invest in their IT infrastructure plus invest in the people who are supporting their business.

For future work, it may be useful to compare SNORT and pfSense experiments and their simulations, using a similar controlled setup within the same environment of the SME, for example, in the office environment or fully from the home environment. This will provide perspectives on better comparisons and relative conclusions based on this study rather than in the disruption of the global pandemic that was experienced in 2020.

As it stands, businesses and organisations, with the help of government policies and processes, will use this balancing act to combat hackers, malicious actors and their bots and manage the best they can to stay ahead of the game. These SMEs could also benefit from having their business participate in models such as SMECRA to understand where these SMEs are in terms of their long-term IT security plans. In future work, it would be good to discuss the privacy and security issues faced by SMEs rising from the challenges of operating in a COVID-19 environment such as remote working from home.

Finally, this is in line with the overall ongoing research that is seeking to explore, both empirically as well as in scenario analysis for different dimensions, the nature and context of cybersecurity. SMEs in the current world of internet and cyber connections also need to find a balance between technology and cost in order for them to see growth.

Author Contributions: Conceptualization, N.R. and A.J.; methodology, N.R. and A.J.; software, N.R.; validation, N.R.; formal analysis, N.R.; investigation, N.R. and A.J.; writing—original draft preparation, N.R. and A.J.; writing—review and editing, N.R., A.J., E.P. and C.H.; visualization, N.R. and E.P.; supervision, A.J. and E.P.; funding acquisition, A.J. and E.P. All authors have read and agreed to the published version of the manuscript.

Funding: This paper has been supported by the KESS2, Knowledge Economy Skills Scholarships and Cardiff School of Technologies—Cardiff Metropolitan University.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

SME	Small and Medium Enterprises
NIDS	Network Based Intrusion Detection System

References

1. Zarpelão, B.B.; Miani, R.S.; Kawakani, C.T.; de Alvarenga, S.C. A survey of intrusion detection in Internet of Things. *J. Netw. Comput. Appl.* **2017**, *84*, 25–37. [CrossRef]
2. O'Leary, D.E. 'Big Data', the 'Internet of Things', and the 'Internet of Signs'. *Intell. Syst. Account. Financ. Manag.* **2013**, *20*, 53–65. [CrossRef]
3. Gartner. 2020. Available online: https://www.gartner.com/en/information-technology/glossary/big-data (accessed on 16 October 2020).
4. Cox, M.; Ellsworth, D. Managing Big Data for Scientific Visualization; ACM Siggraph: 1997. Available online: https://www.researchgate.net/profile/David-Ellsworth-2/publication/238704525_Managing_big_data_for_scientific_visualization/links/54ad79d20cf2213c5fe4081a/Managing-big-data-for-scientific-visualization.pdf (accessed on 15 January 2020).
5. Ashton, K. That 'Internet of Things' Thing. 2009. Available online: http://www.rfidjournal.com/article/view/4986 (accessed on 15 January 2020).
6. Hernandez, P. App Employs Context for Big Dataanalytics Efficiency, Enterprise Apps Today, 18 September 2012. Available online: http://www.enterpriseappstoday.com/businessintelligence/app-employs-context-for-big-data-analyticsefficiency.html (accessed on 15 January 2020).

7. Machanavajjhala, A.; Reiter, J.P. Big privacy: Protecting confidentiality in big data. *XRDS Crossroads ACM Mag. Stud.* **2012**, *19*, 20–23. [CrossRef]
8. Iman, R.N.; Asmiyanto, T.; Inamullah, M.H. Users' Awareness of Personal Information on Social Media: Case on Undergraduate Students of Universitas Indonesia. *Libr. Philos. Pract.* **2020**, 4473. Available online: //core.ac.uk/download/pdf/345183285.pdf (accessed on 21 July 2021).
9. Sardi, A.; Rizzi, A.; Sorano, E.; Guerrieri, A. Cyber Risk in Health Facilities: A Systematic Literature Review. *Sustainability* **2020**, *12*, 7002. [CrossRef]
10. Dunham, K.; Melnick, J. *Malicious Bots: Aninside Look into the Cyber-Criminal Underground of the Internet*; CRC Press: Boca Raton, FL, USA, 2008.
11. Gallaher, M.P.; Link, A.N.; Rousers, B. *Cybersecurity: Economic Strategies and Public Policy Alternatives*; Edward Elgar Publishing: Cheltenham, UK, 2008.
12. Preuveneers, D.; Joosen, W. Sharing Machine Learning Models as Indicators of Compromise for Cyber Threat Intelligence. *J. Cybersecur. Priv.* **2021**, *1*, 140–163. [CrossRef]
13. Ali, A. Ransomware: A research and a personal case study of dealing with this nasty malware. *Issues Inf. Sci. Inf. Technol.* **2017**, *14*, 87–99.
14. James, D.; Philip, M. A novel anti-phishing framework based on visual cryptography. In Proceedings of the 2012 International Conference on Pousersr, Signals, Controls and Computation, Thrissur, India, 3–6 January 2012; pp. 1–5.
15. McGuire, M.; Dowling, S. Cyber-Crime: A Review of the Evidence. Summary of Key Findings and Implications. Available online: https://www.bl.uk/britishlibrary/~{}/media/bl/global/social-welfare/pdfs/non-secure/c/y/b/cyber-crime-a-review-of-the-evidence-chapter-1-cyberdependent-crimes.pdf (accessed on 16 October 2020).
16. Conteh, N.Y.; Schmick, P.J. Cybersecurity: Risks, vulnerabilities, and countermeasures to prevent social engineering attacks. *Int. J. Adv. Comput. Res.* **2016**, *6*, 31. [CrossRef]
17. Patrick McCarthy, Patrick McCarthy 2017. Available online: magazineGrid.com (accessed on 15 January 2021).
18. General Data Protection Regulations (GDPR). Available online: https://ico.org.uk/for-organisations/guide-to-dataprotection/guide-to-the-general-data-protectionregulation-gdpr/ (accessed on 16 October 2020).
19. EasyJet. 2020. Available online: https://www.bbc.co.uk/news/technology-52722626 (accessed on 16 October 2020).
20. NHS. Available online: https://www.bbc.co.uk/news/health-39899646 (accessed on 16 October 2020).
21. Fruhlinger, J. Top Cybersecurity Facts, Figures and Statistics. Available online: https://www.csoonline.com/article/3153707/topcybersecurity-facts-figures-and-statistics.html (accessed on 16 October 2020).
22. Finnerty, K.; Fullick, S.; Motha, H.; Shah, J.N.; Button, M.; Wang, V. *Cyber Security Breaches Survey 2019*; Department for Digital, Culture, Media & Sport: London, UK, 2019.
23. Rawindaran, N.; Prakash, E.; Jayal, A. *Management Information Systems and Cyber Security in Government, Public and Private Institutions: Comparison of Developing and Developed Countries*; Cardiff Metropolitan University: Cardiff, UK, 2020; Available online: https://figshare.cardiffmet.ac.uk/AMI2020 (accessed on 17 May 2020).
24. Global Market Insight. 2019. Available online: https://www.globenewswire.com/newsrelease/2019/03/26/1767329/0/en/Intrusion-Detection-Prevention-System-Market-to-hit-8bn-by-2025-Global-Market-Insights-Inc.html (accessed on 20 October 2020).
25. Perens, B. The open-source definition. *Open Sources Voices Open-Source Revolut.* **1999**, *1*, 171–188.
26. ZDNet. 2020. Available online: https://www.zdnet.com/article/its-an-open-source-world-78-percent-of-companies-run-open-source-software/#:~{}:text=The%20good%20news%20is%20that,%2C%2078%20percent%2C%20of%20businesses.&text=This%20statistic%20has%20nearly%20doubled,business%20or%20their%20IT%20environments (accessed on 1 March 2020).
27. Anderson, J.P. *Computer Security Threat Monitoring and Surveillance*; Technical Report; James P Anderson Co.: Fort Washington, PA, USA, 1980.
28. Spafford, E.H. The Internet Worm Program: An Analysis. *ACM Comput. Commun. Rev.* **1989**, *19*, 17–57. [CrossRef]
29. Garcia-Teodoro, P.; Diaz-Verdejo, J.; Maciá-Fernández, G.; Vázquez, E. Anomaly-based network intrusion detection: Techniques, systems, and challenges. *Comput. Secur.* **2009**, *28*, 18–28. [CrossRef]
30. Scarfone, K.; Mell, P. *Guide to Intrusion Detection and Prevention Systems (IDPS)*; Recommendations of the National Institute of Standards and Technology; National Institute of Standards and Technology: Maryland, MA, USA, 2007.
31. Cisco. 2020. Available online: https://www.cisco.com/c/en/us/td/docs/security/firepousersr/620/configuration/guide/fpmc-config-guidev62/working_with_intrusion_events.html (accessed on 15 January 2020).
32. Bhushan, K.; Gupta, B.B. Distributed denial of service (DDoS) attack mitigation in software defined network (SDN)-based cloud computing environment. *J. Ambient Intell. Humaniz. Comput.* **2019**, *10*, 1985–1997. [CrossRef]
33. Howser, G. The OSI Seven Layer Model. In *Computer Networks and the Internet*; Springer: Cham, Switzerland, 2020; pp. 7–32.
34. Kabiri, P.; Ghorbani, A.A. Research on intrusion detection and response: A survey. *IJ Netw. Secur.* **2005**, *1*, 84–102.
35. Mukherjee, B.; Heberlein, L.T.; Levitt, K.N. Network intrusion detection. *IEEE Netw.* **1994**, *8*, 2641. [CrossRef]
36. Innella, P.; McMillan, O. An Introduction to Intrusion Detection Systems. 2001. Available online: www.symantec.com/connect/articles/introduction-ids (accessed on 16 October 2020).
37. Injadat, M.; Moubayed, A.; Nassif, A.B.; Shami, A. Multi-stage optimized machine learning framework for network intrusion detection. *IEEE Trans. Netw. Serv. Manag.* **2020**, *18*, 1803–1816. [CrossRef]

38. Brown, R.J.; Hewage, C.; Jayal, A. "Breaking and Entering": Evaluation of the Use of Machine Learning for Code Breaking. Available online: https://www.researchgate.net/profile/Chaminda_Hewage/publication/327655930_BREAKING_AND_ENTERING_EVALUATION_OF_THE_USE_OF_MACHINE_LEARNING_FOR_CODE_BREAKING/links/5b9c04cc92851ca9ed0a9be8/BREAKING-AND-ENTERING-EVALUATION-OF-THE-USE-OF-MACHINE-LEARNING-FOR-CODE-BREAKING (accessed on 15 January 2020).
39. Hewage, C.; Jayal, A.; Jenkins, G.; Brown, R.J. A Learned Polyalphabetic Decryption Cipher. Available online: https://www.researchgate.net/publication/330244560_A_Learned_Polyalphabetic_Decryption_Cipher (accessed on 15 January 2020).
40. Belgrana, F.Z.; Benamrane, N.; Hamaida, M.A.; Chaabani, A.M.; Taleb-Ahmed, A. January 2021. Network Intrusion Detection System Using Neural Network and Condensed Nearest Neighbors with Selection of NSL-KDD Influencing Features. In Proceedings of the 2020 IEEE International Conference on Internet of Things and Intelligence System (IoTaIS), Bali, Indonesia, 27–28 January 2021; pp. 23–29.
41. Di Mauro, M.; Galatro, G.; Fortino, G.; Liotta, A. Supervised feature selection techniques in network intrusion detection: A critical review. *Eng. Appl. Artif. Intell.* **2021**, *101*, 104216. [CrossRef]
42. Machine Learning in Cyber Security Domain—7: IDS/IPS with ML. Available online: https://www.normshield.com/machinelearning-in-cyber-security-domain-7-idsips-with-ml/ (accessed on 15 January 2020).
43. Estevez-Tapiador, J.M.; Garcia-Teodoro, P.; Diaz-Verdejo, J.E. Anomaly detection methods in wired networks: A survey and taxonomy. *Comput. Commun.* **2004**, *27*, 1569–1584. [CrossRef]
44. Denning, D.E.; Neumann, P.G. *Requirements, and Model for IDES—A Real-Time Intrusion Detection System*; Technical Report 83F83-01-00; Computer Science Laboratory, SRI International: Menlo Park, CA, USA, 1985.
45. Denning, E.D. An intrusion-detection model. *IEEE Trans. Softw. Eng.* **1987**, *13*, 222–232. [CrossRef]
46. SNORT WEBSITE Reference. Available online: https://www.snort.org/ (accessed on 15 January 2020).
47. Patel, K.C.; Sharma, P. A Review paper on pfSense—An Open-source firewall introducing with different capabilities customization. *IJARIIE* **2017**, *3*, 2395–4396.
48. Marinova-Boncheva, V. A short survey of intrusion detection systems. *Probl. Eng. Cybern. Robot.* **2007**, *58*, 23–30.
49. Lee, J.; Pak, J.; Lee, M. October. Network Intrusion Detection System using Feature Extraction based on Deep Sparse Autoencoder. In Proceedings of the 2020 International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Korea, 21–23 October 2020; pp. 1282–1287.
50. Armenia, S.; Angelini, M.; Nonino, F.; Palombi, G.; Schlitzer, M.F. A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. *Decis. Support Syst.* **2021**, *147*, 113580. [CrossRef]
51. Ahmed, N.N.; Nanath, K. Exploring Cybersecurity Ecosystem in the Middle East: Towards an SME Recommender System. *J. Cyber Secur. Mobil.* **2021**, *10*, 511–536.
52. Mansfield, M. Cyber Security Statistics: Numbers Small Businesses Need to Know. Available online: https://smallbiztrends.com/2017/01/cyber-security-statistics-small-business.html (accessed on 21 July 2021).
53. Kothari, C.R. *Research Methodology: Methods and Techniques*; New Age International: Delhi, India, 2004.
54. Cisco. 2020. Available online: https://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generationfirewalls/datasheet-c78-733916.html (accessed on 15 January 2020).
55. Cisco. 2020. Available online: https://blogs.cisco.com/security/anomaly-vsvulnerability-detection-using-cisco-ips (accessed on 15 January 2020).
56. Patel, A.; Qassim, Q.; Wills, C. A survey of intrusion detection and prevention systems. *Inf. Manag. Comput. Secur.* **2010**, *18*, 277–290. [CrossRef]
57. Roesch, M. Snort: Lightweight intrusion detection for networks. *Lisa* **1999**, *99*, 229–238.
58. Steve Gantz. 2016. Available online: https://www.youtube.com/watch?v=RwWM0srLSg0 (accessed on 20 March 2020).
59. Sönmez, F.Ö.; Günel, B. Evaluation of Security Information and Event Management Systems for Custom Security Visualization Generation. In Proceedings of the 2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT), Ankara, Turkey, 3–4 December 2018; pp. 38–44.
60. *Algorithms in C: Fundamentals, Data Structures, Sorting, Searching, Robert Sedgewick*; Addison-Wesely Publishing Company, Melbourne Wesley Cummings: Beverly, MA, USA, 1997.