National College of Ireland

Comparative Analysis of Cybersecurity Solutions and how an Organisation should Prioritise these Solutions

MSc Research Project in Cyber Security

Nathan Kelly
Student ID: x20211261

School of Computing
National College of Ireland

Supervisor: Ross Spelman

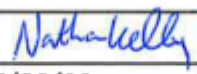
National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Nathan Kelly
Student ID:	X20211261
Programme:	Computer and Security Software
Year:	2022
Module:	MSc Research Project
Lecturer:	Mr. Ross Spelman
Submission Due Date:	15/08/22
Project Title:	Comparative Analysis of Cybersecurity Solutions and how an Organisation should prioritise these Solutions
Word Count:	8940
Page Count:	20

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	
Date:	15/08/22

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Comparative Analysis of Cybersecurity Solutions and how an Organisation should prioritise these Solutions

Nathan Kelly
X20211261

Abstract

Money is everything in modern day business. Organisations want to increase their profits, but they also want to limit their spending at the same time. How can this be achieved? Unfortunately, there is no magic formula. Covid-19 meant that many organisations had to adapt fast to stay afloat, as employees working from home suddenly became the norm. In order to accommodate this, money needed to be spent to improve the security status of their employees' corporate laptops and mobile devices. But this was not all, suddenly solutions that were not at the latest version needed to be upgraded or reviewed- and fast. Multi-Factor authentication had to be enabled, Anti-Virus or EDR software had to be upgraded, Encryption had to be rolled out to all devices. This was just the start! Other organisations went further again, spending substantially to implement new cybersecurity solutions which could help secure their network. Controls like SIEM solutions, Vulnerability Management scanners, and Open-Source Intelligence tools became big business. But where should an organisation draw the line with these security controls? The attack on the HSE showed what a massive problem it is trying to get the right levels of security in place. Cybersecurity budgets are limited, so can businesses get away with implementing just one or two of these solutions? If so, which tools or solutions are the most effective in protecting an organisation from the threat of cyber-crime? These are not easy questions to answer, even cyber-security experts will argue for one control over another. So, what hope does a CEO or board of directors have of making an informed decision on this? Is there some way that they could effectively employ an evaluation table or matrix to analyse and compare different cybersecurity solutions, and at the same time be given an idea of which of these should be prioritised? If so, this could save their organisation millions. In this research paper I investigate and demonstrate how to assist an organisation in evaluating what cybersecurity controls are "must-haves," what are "nice-to-haves," and what are not worth the effort of implementing- as well as categorising these into different levels of prioritisation.

Contents table

1. Introduction 5

1.1 Background of Problem 5

1.2 Research Question and Objectives 6

1.3 Structure of Report 6

2. Literature Review 7

2.1 Choice of topic and early reading 7

2.2 Significance of study 8

2.3 Related Work 8

3. Research Methodology 9

3.1 Requirements 9

3.2 Process and Design 9

3.3 Data Collection 10

3.4 Comparative Analysis 10

3.5 Description of Cyber Security Solutions 10

3.6 Time-Management 11

3.7 Discussion 12

4. Design Specifications 12

4.1 Design Specification 12

4.2 Assumptions made 12

4.3 Data Points 13

4.4 Metrics 14

5. Implementation 15

5.1 Implementation Specification 15

5.2 Implementation of Scores into Matrix 16

6. Evaluation 16

6.1 Comprehensive Analysis of Business Value scoring 16

6.2 Comprehensive Analysis of Complexity scoring 18

6.3 Prioritisation of Cybersecurity Solutions 19

6.4 Critical Analysis and Implications 20

7. Conclusion and Future Work 21

8. Acknowledgement 22

9. References 23

1. INTRODUCTION

Within this introduction, I will outline the background of the problem, the research question, and my objectives. I shall also discuss the problem statement, the potential solution statement, as well as the motivation and necessity to solve this problem. Finally, I will provide an overview of the structure of the project and summarise each of the different sections of the report.

1.1 Background of Problem

It is the job of the CEO to make the big decisions within an organisation. This is the reason why they are paid the large salaries and given so much trust. But it is not enough to just make the decisions, they need to make the *correct* decisions. It is statistically proven that CEO's make mistakes when making decisions around cybersecurity. "Executives are more often than not complacent with cyber, especially when looking at the number of organisations that have failed to implement what we believe are cyber basics". (TechCentral.ie, 2018) But making the right choices is easier said than done. Selecting the right cybersecurity controls is a big problem and making a mistake with this could end up costing them more than just money. One of the biggest issues a CEO faces is understanding the risk/reward. If an organisation knew how much value they were getting from specific security controls, this would allow them to make more informed decisions. So how can we help them identify what cybersecurity solutions are the most important to their business, and when working off a limited budget- which of these solutions should be prioritised?

The benefits to an organisation of getting these decisions right, are obvious. They would result in:

- ✓ a more secure network
- ✓ enhanced mitigation against risks
- ✓ better protection against both internal and external threats
- ✓ better compliance scores
- ✓ improved brand trust and reputation
- ✓ increased productivity
- ✓ cost savings and value

Needless to say, when implementing any cybersecurity solution, there are potential downsides. If the solution does not fit with the business, then this expensive cybersecurity control may be of little or no benefit, depending on the product and the nature of the organisations business.

So, the main motivation of this project is to investigate what can be done to assist an organisation when making big financial decisions based around cybersecurity budgets (Rinaldi, 2020), and what cybersecurity solutions should be implemented and prioritised along the way. How important is a SIEM solution compared to Vulnerability Management scanning? How does Endpoint Detection and Response match up against Open-Source Intelligence tools when scored against each other?

The beneficiaries from this research project should be widespread, not just academically but also within industry. Any organisation who are looking to implement a new cybersecurity solution could use this as a

guidance, or even just a back-up to help them validate their decision. It could also assist in identifying what other cybersecurity solutions should follow on from there.

1.2 Research Question and Objectives

The broad area of my research question is Computer and Software Security under the wider Cyber Security umbrella. The title of my research project offers a general overview of what I aim to achieve in this project. A more defined research question or problem statement for this research project might be "How is it possible to help an organisation evaluate different cybersecurity solutions, and demonstrate how these solutions should be prioritised?"

During the evaluation phase I will also address questions like: "How can I help demonstrate how much value a cybersecurity solution will bring to an organisation?" As a solution statement, I believe that by identifying a number of explicit data points and evaluating a cybersecurity control based on these, then any cybersecurity solution could then be measured and evaluated against any other. From these data points, we can get metrics for both Business Value and Complexity, which will then allow us to prioritise these cybersecurity solutions within an organisation. The creation of evaluation tables or matrices have been done before in other research papers, but what is unique about my research project is that I am trying to create an evaluation and prioritisation method of comparing totally different cybersecurity solutions.

My first objective was to come up with a number of data points which are relevant and measurable to a wide and contrasting range of cybersecurity solutions. For this research project I decided to focus on four differing cybersecurity solutions, but my aim is that any other cybersecurity solution can be plugged into my metrics table and measured against the same data points. Objective#2 was to score these four cybersecurity solutions against the data points to give two different bottom line scores, one for Business Value and one for Complexity. Whatever cybersecurity solution scores highest in this Business Value assessment is the one we are anticipating delivering the most value to the organisation. Then, using these two values along with a separate model we can decide on which solution should be prioritised over the other. Objective#3 was to compare my scoring results against the results of my online survey to see if the prioritisation of the tools was similar or if there was any disconnect between my findings and the opinions of the participants of my online survey.

1.3 Structure of Report

- Section 2 is the Literature Review where I will demonstrate some evidence of my independent research and discuss how I ended up deciding what direction to go with the research project.
- Section 3 of the report outlines my Research Methodology, where I discuss the methods of any actions carried out throughout the project. This includes references to my online survey, my evaluations, and my time management throughout the course of the project.
- Section 4 entitled Design Specifications shows the techniques and framework used for the implementation. I discuss what I want to do with my scores for Business Value and Complexity and how they will fit into the prioritisation matrix. I also discuss the data points in further detail and the assumptions made on the fictional company I am basing the work off. Finally, I go through my metrics and how the scoring mechanism will work for each data point.

- Section 5 describes the final stages of the implementation.
- Section 6 is the Evaluation section where I look at a comprehensive analysis of the results and main findings of the study, and my online survey, as well as the implications of these findings. This section contains the scoring tables for both Business Value and Complexity with some detail on how scores were achieved. It finishes by displaying the Business Value Vs Complexity matrix and where each cybersecurity solution sits within that.
- In my conclusion I examine the results obtained compared to my original objectives. I also look further at the implications and limitations of this project and make some suggestions and proposals for further research in this area.

2. LITERATURE REVIEW

In this literature review section, I will discuss my choice of topic and reference some previous research done in this area. I have included references to the literature review from my previous literature review work in the "Research in Computing" module as I felt that this too was relevant to this project.

2.1 Choice of topic and early reading

My previous literature review work conducted as part of Research in the Postgraduate Diploma was focussed purely on the advantages of having a Security Information Event Management (SIEM) Security Operations Centre (SOC) in place for an Irish Financial Services Organisation, so I had done a lot of reading in this particular area. However, I felt it would be difficult to submit a thesis on the same subject matter since I had exhausted many possibilities and ran into some dead ends by the end of that literature review work. After much careful consideration I decided it would be intriguing to expand my horizons for this research project to include some additional cybersecurity controls and try to come up with some metrics on each of these. This might help an organisation trying to identify the value they would get from a particular cybersecurity solution. So, with guidance from my supervisor, the decision was made to modify my research project and widen the range of cybersecurity solutions involved.

In trying to decide what solutions I should focus on, I researched many cybersecurity solutions and tools. I sought strong standalone solutions, ones not overly reliant on other security controls around them. Although this can only be true to a point. As an example, if the servers (or systems producing the logs across the business) are not in good health then it would be difficult to get relevant security logs from these which could then be analysed within the SIEM. But assuming a healthy infrastructure estate within the organisation I wanted to discover cybersecurity solutions which could then be introduced to enhance the security of the network and organisation as a whole.

As mentioned above, having already focussed previously on the benefits of a **Security Information Event Management or SIEM,** this cybersecurity solution was an obvious option for me again in this research project. Finding the other cybersecurity solutions would take more time, but I knew that whatever ones I chose I wanted them to be independent of each other. For example, I did not necessarily want to choose Anti-Virus or Firewall tools as these would typically feed logs into a SIEM if it existed within an organisation.

I spent time speaking to colleagues and classmates about the controls that their Information Security teams used within their organisations. I learned a lot from this and found that although the industries and their subsequent governing rules can be quite different, that the fundamentals remain the same. Many of them do similar things. Cyber criminals will almost always perform reconaissance on a network. (Sharpe, 2022) The end game here is to see if they can identify any vulnerabilities in a network. So from the outside they are checking and probing IP ranges, scraping email addresses from websites and doing what they can to get access. With this in mind, I decided that an **Open Source Intelligence tool (OSINT)** should be considered in my research project for those hackers trying to get access externally. Then, if we were to assume that a hacker has already infiltrated a network and is working from the inside, then internal **Vulnerability Management scanning** would be another important solution to consider for the research project.

The final cybersecurity solution that I chose is arguably the most obvious, and is the one that people would be most familiar with. **Endpoint Detection and Response (EDR)** is seen by many as the evolution of Anti-Virus products. (Samson, 2022) Contrary to my earlier statement, Anti-Virus is something that would feed logs into a SIEM, and EDR would do similar once configured, however it offers much more interactive security functionality in its own right, and because of this I felt it was a strong option to be considered. So in summary, the four cybersecurity solutions chosen would all be popular and widely used amongst Information Security teams across the country, and around the world. (Sapphire, 2022)

2.2 Significance of study

The issue I aim to address is significant in the field as it is a problem faced by CEO's and organisations around the world on a daily basis. "How can I evaluate one cybersecurity control against another?" In my previous role as Information Security Analyst at my current company, I was tasked with the job of setting up a SIEM solution within the organisation. This was the first dedicated cybersecurity solution that I worked on and was the second introduced to the business (after EDR) Once this had been implemented, myself and my manager had to make decisions on what cybersecurity solutions should be implemented next within the business. There were many considerations that we needed to take onboard as part of this project. At the time we were operating within a tight budget with very few resources in terms of experienced IT team members. We needed to put forward a case to the business to show them that the tools we had identified and wanted to onboard, would be beneficial to our business. This was a time-consuming task and I felt that if there was some formula or metrics that we could produce that could be applied to any cybersecurity solution across the board that it would have been extremely useful. So, this idea has been in my head for quite a while, and I felt that having focussed solely on the benefits of a SIEM SOC in the literature review work (conducted as part of Research in Computing module last semester) that this would be an exciting opportunity to see how it might be possible to create something that would be useful both academically and in modern business.

2.3 Related Work

A paper entitled "Cyber Security Solutions for Businesses in Financial Services: Challenges, Opportunities, and the Way Forward" (Akhtar, et al., 2021) was a paper I found during my literature review process and one I found very interesting. In it the authors referred to many challenges that are facing modern businesses

and how a layer security approach can be a strategically smart move. It also discusses how 10-15% of the organisations overall budget should be the bare minimum that the cybersecurity budget should be allocated.

3. RESEARCH METHODOLOGY

My Research Methodology is a general outline of how my research was carried out. It defines the techniques or procedures which were used to identify and analyse information regarding this specific research topic. (Voxco, 2022) Here I discuss my methodological approach to this research project and the decisions that I made along the way. What I researched, how I researched it, why I chose the cybersecurity solutions that I did, and the next steps that are required to bring my research to completion. I also refer to the time management structure that I had in place to try and research, plan, document and finalise everything within the given time period.

3.1 Requirements

Upon beginning this research project, I was aware that I need to meet requirements along the way to be able to succeed in this project. I tried to use these requirements as "journey markers" as the weeks and months passed. I wrote them up on in my research notes and tried to tick them off as I went along. Below is what I had listed:

- ✓ Problem Statement
- ✓ Solution Statement (outlining what I what to demonstrate)
- ✓ Metrics
- ✓ Survey
- ✓ Provide opinion

3.2 Process and Design

The first steps in the process of this research project have already been discussed as part of my literature review above. In trying to decide what solutions I should focus on, I read up on many cybersecurity solutions and tools but ended up choosing the four security solutions below:

- Endpoint Detection & Response (EDR)
- Vulnerability Management Scanning (VM scanning)
- Security Information Event Management (SIEM) solution
- Open Source Intelligence Tools (OSINT)

Once I had decided where to focus my attention, I could then compare these solutions against different data points, showing what they offered to an organisation and finding out how these cybersecurity solutions were viewed by different levels of employee across the workplace. This would produce results which I could then compare to the results of my online survey to see how tuned in people are to the strengths and weaknesses of cybersecurity controls. From this point on in my report I will refer to Endpoint Detection and Response as "EDR", Security Information Event Management as "SIEM," Vulnerability Management as "VM scanning" and Open-Source Intelligence tool as "OSINT".

Next was my design stage where I had to come up with some metrics around how these cybersecurity solutions could be measured. Initially, I had some difficulty trying to come up with a formula which would encompass all of the data points which I wanted to include. I tried evaluating each of the solutions against the data points with scores of high, medium, or low, however this did not give me any clear output in terms of bottom-line scoring- so I decided to go with a points-based system which I shall go into in greater details later in this report.

3.3 Data Collection

The data collection process for this research project was a long and drawn out process. It involved the creation of an online survey which was sent directly out to some of my work and college colleagues from the past and present. I used Google Forms to create this survey and set up several test surveys beforehand to ensure that I got the look and feel of it right. I also tried to ensure that I was asking the right questions, so that there were useful answers coming back. Prior to the release of this survey, the relevant ethics forms were filled out and submitted as required. Once the survey was released, the responses were slow to come back, and so after a few days I decided to post it onto Linkedin in a bid to get some more participants. My target was to get 50 participants and I exceeded this figure getting a total of 52 responses.

This online survey focussed on getting the participants views on various cybersecurity controls. It was not a technical survey but rather asked the participant if they were aware of cybersecurity controls within their workplace, what they controls were, and if the participant knew what these controls did and how much effort was involved in managing them. Full details of these questions and their responses can be found in my configuration manual.

3.4 Comparative Analysis

In order to be able to do a comparative analysis of the cybersecurity solutions, it was necessary to identify several data points that these solutions could be scored against. The purpose of these data points was to measure the value of the cybersecurity solution to the business- by listing some benefits that it would provide- and to measure the complexity of the solution- by analysing how it fits into the network infrastructure. These data points are discussed further in Section 4, Design Specifications.

3.5 Description of Cyber Security Solutions

Below is a brief description of each of the four cybersecurity solutions involved in this research project including some commonly used examples of each.

3.5.1 Endpoint Detection & Response (EDR)

EDR is “an integrated endpoint security solution that combines real-time continuous monitoring and collection of endpoint data with rules-based automated response and analysis capabilities.” (Trellix, 2022) It would typically be installed onto all endpoints (laptops and servers) within an organisation and would incorporate anti-virus and other endpoint security functionality to provide more fully featured protection against a wider range of cyber threats. (Checkpoint, 2022) Examples of EDR products would be Checkpoint Sandblast or Microsoft Defender for Endpoints.

3.5.2 Vulnerability Management Scanning (VM scanning)

Vulnerability scanners are valuable tools that search for, and report on, the known vulnerabilities within the IT infrastructure/network of an organisation. (Coresecurity, 2022) In this case we are referring to vulnerability scanning from inside the network rather than externally. When run from inside a network they can reveal large numbers of vulnerabilities which could be exploited if a hacker had already infiltrated an organisation's infrastructure. Examples of Vulnerability scanning tools would be Nessus, Qualys, OpenVAS, Tenable and Nmap.

3.5.3 Security Information Event Management (SIEM) solution

A SIEM is a software solution that collects and analyses activity from many different resources across an entire IT infrastructure. It gathers security logs and data from all devices within the network, such as servers, firewalls, domain controllers, and Anti-Virus or EDR solutions, to name just a few. The SIEM will store, normalise, aggregate, and then apply analytics to that data to discover trends, detect threats, and empower organizations to investigate any alerts. (Petters, 2020) Best known examples of these would be QRadar or Splunk.

3.5.4 Open-Source Intelligence Tools (OSINT)

OSINT focusses on publicly accessible, external data sources when performing assessments. They are useful tools as they can show you a "hackers-eye" view of your systems, allowing you to identify particular areas of weakness and put plans in place to mitigate these. They would often provide a scoring system for different areas of a network and provide recommendations on what should be addressed as high, medium, or low level or urgency. Examples of OSINT tools would be Black Kite or RiskRecon.

3.6 Time-Management

Below is an approximate timeline of how I managed my time throughout this research project from the initial decision on the research question through to the final reporting writing and preparation for the video presentation.

	April				May				June				July					August	
	04-10	11-17	18-24	25-01	02-08	09-15	16-22	23-31	01-05	06-12	13-19	20-26	27-03	04-10	11-17	18-24	25-31	01-07	08-14
Consideration of Research Question																			
Literature Review																			
Data collection & Analysis																			
Report Writing																			
Video Presentation																			

3.7 Discussion

As the research project progressed through its stages, many additional questions needed to be considered. Some of these I have tried to encapsulate into this project, but others would require more time to be spent on them in order to gain a fuller understanding.

- What other cybersecurity solutions could I have selected?
- Are my data points a true and fair measure of how these solutions should be measured?
- What other data points would be useful to measure and compare cybersecurity solutions?
- What other formula or metrics could be used to evaluate these solutions?
- How different would my survey results have been if directed to cybersecurity professionals only?

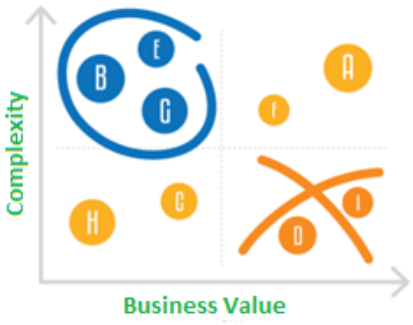
4. DESIGN SPECIFICATIONS

4.1 Design Specification

In this section, the techniques and framework that underlie the implementation are identified and presented. The data points which were used to measure the four cybersecurity solutions are also listed and explained.

My research project objective is to help organisations evaluate certain cybersecurity solutions, but as well as that, I wanted to identify which of the solutions should be prioritised or implemented first. In order to help achieve this I chose to use the "Value vs Complexity Matrix." (Mahajan, 2016) This allowed me to evaluate each of the cybersecurity solutions according to how much value they would bring to the organisation versus how complex they would be to implement. "Value V Complexity is a prioritisation model that organisations use to prioritise initiatives on a roadmap. It is a popular way to look for an objective method of allocating time and finite developments resources to initiatives based on their perceived or potential benefit to a company". (ProductPlan, 2022) So, although I will be using this matrix to help identify which of the cybersecurity solutions should be prioritised, I will be using my own metrics and scoring to determine what score each of these solutions get in terms of value and in terms of complexity.

Here is a sample of a Business Value V Complexity matrix which will show where our solutions might fit. The various solutions will fit in different sections of the grid depending on their evaluations. As we can see, the X-axis represents Business Value, and the Y-axis represents Complexity. (ProductPlan, 2022)



4.2 Assumptions made

For the purpose of this research project, I am pertaining to work for a fictional organisation whose board of directors and external auditors have instructed that they need to implement some cybersecurity controls for regulatory purposes, as well as for their fear of a cyberattack. Using my metrics and processes, this Irish Financial Services company want to implement some security controls as soon as possible, however they have a limited budget and no idea where to start the process. This organisation has approximately 150 employees (50 of whom work from home) and each employee has their own laptop. The company has 50

servers in total of all descriptions, including Web servers, Application servers, Email servers, File servers, Database servers, DNS servers, DHCP servers, SFTP servers and Proxy servers. So, in total 150 laptops plus 50 servers make 200 endpoint devices. Given that this company, by the name of "Big Red Insurance" are a financial services company, they would then come under the guidelines of the Central Bank of Ireland (CBI). These stringent restrictions are another one of the main reasons for the organisation having to decide what cybersecurity solutions to onboard. The data used to create this fictional organisation is based on an average financial services company within Ireland. (IDA Ireland, 2022)

It was assumed when comparing these cybersecurity solutions that each of them would have 100% coverage across the network. This meant that all possible logs were set up to report to the SIEM, that all devices were included in a vulnerability scan, that EDR software was installed on every device on the network and that OSINT had a full view of all discoverable external IP ranges. It is also assumed that basic Anti-Virus software is already established within the organisation already- hence this is not in scope for the project.

4.3 Data Points

In order to be able to quantify the benefits of each of these controls we need to have data points to measure each of them against. These data points are reasons why an organisation might want to implement a cybersecurity solution and should help indicate why one solution should be chosen over another. This list is derived from not only my own research, but from discussions with colleagues who would implement and onboard cybersecurity solutions or other IT software solutions as part of their daily role.

The term "Business Value" in this scenario refers to the value that the cybersecurity solution will provide to the organisation. I have included costs in this section because there are usually strict budgets that need to be considered before implementing any new solution. The following five data points will be used to get an overall score for Business Value:

4.3.1 **Cost to Implement:** How much will it cost to implement this control into the organisation?
4.3.2 **Cost to Maintain:** Once implemented, what will be the annual cost to maintain the solution? This could involve costs for licencing, version updates or patches.
4.3.3 **Reporting Ability:** Does the solution have the ability to provide clear and accurate reports?
4.3.4 **Risk of not having solution in place:** If the organisation does not have this cybersecurity solution in place, then what is the risk for them?
4.3.5 **Regulatory Obligations:** Would the organisation be obliged by CBI rules and regulations to have certain cybersecurity solutions in place?

For reference, the term "Complexity" here refers specifically to how complex the cybersecurity solution is, both in terms of operating it, and also integrating it into the organisation. The following five data points will be used to get an overall score for Complexity:

4.3.6 **Effort to Implement:** How much effort on the part of the organisation and relevant teams needs to go into implementing the solution? How long will it take to have this solution fully onboarded?
4.3.7 **Effort to Maintain:** How many days will the organisation need to spend weekly/monthly to maintain the upkeep of this**?**

4.3.8 Difficulty to Operate: How easy or difficult is the solution to operate? What is the availability of talent to operate this solution?

4.3.9 Operational Impact: Does the solution slow down machines or impact users in any way?

4.3.10 Reliance on other tools: How reliant is this on other cybersecurity solutions or tools which may or may not already exist in the organisation?

Further information on these data points can be found in my accompanying configuration manual.

4.4 Metrics

In order to classify these cybersecurity solutions, I have used Microsoft Excel to build two scoring matrices. One for Business Value and one for Complexity. To summarise once again, the Business Value assessment considers how much value it anticipates the cybersecurity solution to deliver. The Complexity assessment considers how much effort it will take to implement. The aim is to uncover the cybersecurity solutions that promise to deliver the most value for the least effort. Each of these assessments contains five data points with scores ranging from 0-10, where 10 is the most favourable (or optimum) score for the data point, and 0 is the least favourable score.

The full table and breakdown of all the scoring for the solutions against the data points is shown in Section 6 below. The accompanying configuration manual document also gives further detail on the scoring given in the tables.

4.4.1 Scoring mechanism for each data point

In order to be able to analyse what rating each solution would have, I needed to specify a points-based scoring system for each data point. Each of the data points are broken down into different scoring zones and then each solution is graded based on how well or poorly they match up within that data point.

It is important to note that the cost and effort data points outlined below would be variable depending on the scale of the organisation. In a real-life scenario, these metrics could change based on the size of the organisation. However, for the purpose of this research project, these cost and effort data points are being based off the fictional organisation described in section 4.2.

Below is a brief description of the scoring patterns for each of the data points:

- **Cost to Implement:** Based on industry knowledge as well as online research around the costings of each of the solutions, this data point has been broken down into five scoring sections based purely on the cost of implementing the solution into an organisation. The lower the cost, the higher the score rating. If the solution costs less than €2,500 then it will score 10, and the higher the cost is the lower the final score. The reason we chose this figure is that many smaller organisations cyber budgets would be small but would still be able to afford a solution of this cost. (Security Boulevard, 2022)
- **Cost to Maintain:** This data point relates to costs around software updates, patches, or annual licencing fees for each of the solutions. From online research and industry knowledge, the scoring has been divided into five scoring sections based on the cost per annum to maintain the control. Again, for this data point, the lower the cost the better the score rating for the cybersecurity solution.

- **Reporting Ability:** In order for an organisation to get good Business Value out of a cybersecurity solution, the reporting function is critical. It could be the best cybersecurity solution available but without appropriate reports then it is not going to cut it when presented to a board of directors. For this data point, the higher the reporting detail, the higher the score rating.
- **Risk of not having the solution in place:** Often an organisation will want to introduce a new security solution purely to mitigate a certain risk. This is a data point which should always be considered in any analysis. Scoring-wise, the higher the risk of not having this in place, the higher the score rating.
- **Regulatory Obligations:** Any organisation that is governed by the CBI will have certain regulatory obligations around all of their controls. So, any cybersecurity tool or solution which could satisfy a high number of these obligations would obviously score higher in the ratings. Hence the scoring here is 10 for high and 0 for none. Some of the solutions may be halfway and would receive an appropriate score to reflect this.
- **Effort to Implement:** Some of these tools could be rolled out or implemented with little effort whereas others would take a lot of manual work behind the scenes. For the purpose of this research project, this is measured in days to implement, and the scoring is set up against this. For this data point, the more days it takes to implement, the higher the complexity score. For clarity, if it takes 25 days to implement, then it is highly complex, so it scores the max of 10 here. 2 days shows little effort to implement so a lower complexity.
- **Effort to Maintain:** Similar to the above, effort to maintain the solution is based on "man-hours" per month. For this data point, the more man-hours it takes to maintain monthly, the higher the complexity score.
- **Difficulty to Operate:** The more complex a solution is, the greater expertise and more skilled employees will be required to use it. Because of this a "high" rating here will increase the overall complexity score. To clarify, if it scores high here it gets 5 plus the 3 for medium and the 2 for low giving a total of 10 which is the max score.
- **Operational Impact:** The higher the operational impact on the other tools or devices on the network then the more complex the solution is. Hence, a higher score in this would mean a higher complexity rating**.**
- **Reliance on other tools:** The less reliant a cybersecurity solution is on other tools- the less complex it is. If it is heavily reliant on other tools, then that would increase complexity. The scoring is set up to reflect that, and again some solutions may lie halfway between these boundaries.

5. IMPLEMENTATION

5.1 Implementation Specification

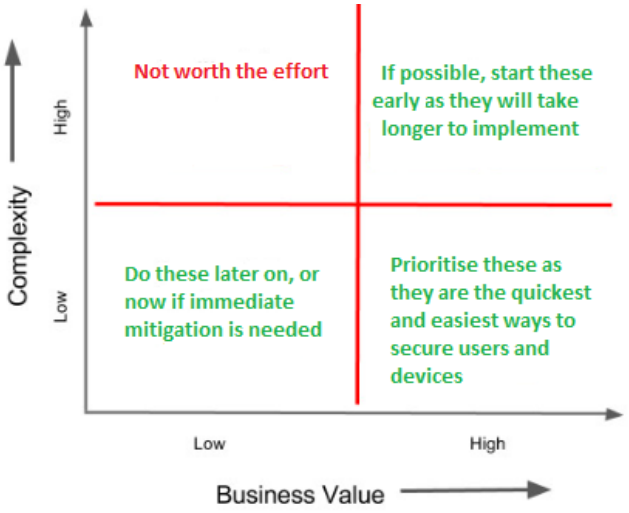
The aim of my metrics is to use my data points to formulate scores for two determining factors, the Complexity of the cybersecurity solution and its Business Value to the company.

- The Business Value score will determine which of the solutions will potentially offer most value to the organisation.
- The Complexity score, along with the Business Value score can then be imported into the Business Value Vs Complexity matrix to reveal where it sits in the grid in terms of prioritisation.

The online survey which I carried out will also provide an insight into how these cybersecurity solutions are viewed within industry, both in terms of importance, and in terms of prioritisation. The process of comparing and contrasting my results against the results of the online survey will give an interesting view on whether the work that I have done aligns with my participants opinions, or whether there is a clear disconnect between what I have shown, and peoples own views or opinions of the cybersecurity solutions.

5.2 Implementation of Scores into Matrix

Summarising each quadrant of the Business Value Vs Complexity matrix (moving from the top-left corner clockwise) – we can see that being placed in the High Complexity/Low Business Value might result in a recommendation to exclude a cybersecurity solution (or at least mean that it is prioritised last) Anything assessed as High Complexity/ High Business Value is certainly worth implementing although- because of its high complexity- it may take a bit longer for this to be completed, so can often be worth beginning the implementation process early before the solutions are required. Low Complexity/High Business Value are win-win for an organisation as they can be implemented fast and offer a lot. Anything in the Low-Low quadrant may need to be reconsidered, to see if it is worth the effort, although if cost is low then this could be another quick-fix to mitigate risk.



6. EVALUATION

In this evaluation section, a comprehensive analysis of the results and main findings of the study as well as the implications of these findings are presented.

6.1 Comprehensive Analysis of Business Value scoring

Below is the excel scoring spreadsheet for each of the cybersecurity solutions. Each data point is worth a maximum of 10, thus the maximum score available is 50. Each cybersecurity solution is scored through the data points with a total score given on the bottom line of the table. The cut-off score is 25, so any solution which scores below 25 will be marked in the “low” quadrant on the X-axis of the grid which represents Business Value. Any solution which scores over 25 will be marked in the “high” quadrant of the X-axis.

The data points are listed along the left-hand side of the table and the cybersecurity solutions being scored are shown along the top. I have used an “x” to highlight the scoring columns that the solution satisfies. In some instances, several boxes will be ticked in the same section, this is because, as an example, if something has high levels of reporting then it would also comply with medium and low levels of reporting so would score the maximum in this case. Comments have also been made within the table giving some overview of

why the score has been decided upon. Further details on these scores can be found in the configuration manual.

*pa= per annum

Cybersecurity Business Value Solution Tender Scoring		Weighting	Endpoint Detection and Response			Vulnerability Management Scanning			SIEM			Open Source Intelligence Tools		
			Detail	Comment	Score	Detail	Comment	Score	Detail	Comment	Score	Detail	Comment	Score
Cost to Implement	Less than €2,500	3		Typically it would take about a calendar month to roll this agent out correctly to 200 devices. So 20days @ €1000 per day			Option to use appliance scanner or agent on each device. Appliance scanner would mean quicker and less costly rollout			Group policy could be set so that endpoints report logs to SIEM. Some servers would need to be manually set up to report logs but overall cost to implement would be high		x	Quick and inexpensive to implement	3
	Less than €10,000	2				x		2				x		2
	Less than €25,000	2	x		2	x		2				x		2
	Less than €50,000	2	x		2	x		2	x		2	x		2
	Less than €75,000	1	x		1	x		1	x		1	x		1
Cost to Maintain	Less than €2,500 pa	3		Cost based on number of endpoints (200) and would be approx €57 per endpoint per year			Cost based on number of endpoints (200) and would be approx €35 per endpoint per year			Cost is based on EPS, so given our number of devices (200) this would be unlikely to exceed €50,000		x	One off cost. Low annual licence fee	3
	Less than €10,000 pa	2				x		2				x		2
	Less than €25,000 pa	2	x		2	x		2				x		2
	Less than €50,000 pa	2	x		2	x		2	x		2	x		2
	Less than €75,000 pa	1	x		1	x		1	x		1	x		1
Reporting Ability	High detail reporting	6	x	Detailed reporting can be seen on a per device basis	6	x	Reporting can contain high detail of vulnerabilities on devices as well as remediations and recommendations	6	x	Can report on every device and show complex details of any issues	6		Reports contain only high-level detail of what can be seen	
	Medium detail reporting	3	x		3	x		3	x		3			
	Low level reporting	1	x		1	x		1	x		1	x		1
Risk of not having solution	High	10	x	EDR should be seen as essential to any organisation	10	x	Moderate risk of not having in place	5	x	Relatively high risk of not having in place	8		No risk of not having this in place	
	None	0										x		
Regulatory Obligations	High	10	x	EDR would satisfy a significant number of regulatory obligations	10		Low regulatory requirements for VM Scanning		x	High regulatory requirements for SIEM	10		Low regulatory requirements for OSINT	
	None	0				x		3				x		3
Total Available Score		50			40			32			34			24

- ✓ From the scoring table above, we can see that EDR scored highest across the five data points with 40 from a possible 50 (or 80%). This would mean that EDR is evaluated as having the highest business value to an organisation. This result is as one might expect given that Anti-virus is the one cybersecurity tool that all businesses would have in place, and EDR is seen as a more evolved version of this. 79% of survey participants chose EDR as a "must have" solution showing that my metrics and the results of my online survey are perfectly in-check.
- ✓ SIEM comes in at second place in the evaluation table with a score of 34, or 68%, suggesting that this would be the next most beneficial cybersecurity solution for "Big Red Insurance". Its major fall-down is its pricing as it can be expensive to implement and maintain as one might expect for such a sophisticated cybersecurity solution. 64% of survey participants saw a SIEM as a "must-have" cybersecurity solution. Those surveyed thought that the SIEM should be prioritised in 3rd place behind EDR and VM scanning.
- ✓ Vulnerability Management scanning scores 32 across the data points (64%), falling down primarily on regulatory obligations. However, this is still a strong score and would encourage an organisation to implement this depending on the size of the budget. Of those surveyed, 67% believed that VM scanning was a "must-have" solution.
- ✓ OSINT, which is the least expensive product, comes in with a score of 24 (48%)- suggesting that its value to an organisation would be considerably less than the other products. 21% of those surveyed believed OSINT was a "nice-to-have" with another 25% saying they would "prefer-to-have" this solution in place. Only 21% in total saw it as a "must-have." This shows that the perception of this cybersecurity solution is broadly in line with its value to an organisation.

To summarise this, my metrics have assessed these cybersecurity solutions and the one with the most Business Value (according to our calculations) is EDR. In second place is the SIEM solution closely followed by Vulnerability Management, very similar to my survey results as we can see in the two tables below. This data shows that I am broadly in line with the survey participants in terms of the Business Value of these cybersecurity controls.

Business Value (from my Metrics)	%
EDR	80
SIEM	68
VM Scanning	64
OSINT	42

Online Survey (perceived as must-have)	%
EDR	78.8
VM Scanning	67.3
SIEM	63.5
OSINT	42

6.2 Comprehensive Analysis of Complexity scoring

Below is the excel scoring spreadsheet for each of the cybersecurity solutions. As with the above, the maximum score available is 50. The cut-off score is 25, so any solution which scores below 25 will be marked in the "low" quadrant on the Y-axis of the grid, which represents Complexity.

				Endpoint Detection and Response			Vulnerability Management Scanning			SIEM			Open Source Intelligence Tools		
Cybersecurity Complexity Solution Tender Scoring			Weighting	Detail	Comment	Score	Detail	Comment	Score	Detail	Comment	Score	Detail	Comment	Score
	Effort to Implement	25 Days	5	x	Can be cumbersome to roll out to endpoints if trying to avoid downtime and keep operational impact low	5		Appliance scanner to be set up or agent rolled out to all endpoints		x	Considerable effort to implement as all log sources need to be set up to report logs	5		Once the domain names are known then little or no effort required to implement	
		10 Days	3	x		3	x		3	x		3			
		2 Days	2	x		2	x		2	x		2	x		2
	Effort to Maintain	10+ man hrs per month	5		1-2 hours maintenance per week would typically cover requirements			Need to ensure any added or removed endpoints are updated prior to scan			Log sources occassionally stop reporting and may need to be looked at.			Recalibration of results may be required but still little effort to maintain	
		5 man hrs per month	3	x		3	x		3	x		3			
		2 man hrs per month	2	x		2	x		2	x		2	x		2
	Difficulty to Operate	High	5	x	From an admin level this needs to be managed carefully to avoid downtime	5		Not overly difficult to operate as once implemented it is often just click of a button to run scan			Once implemented this is relatively easy to operate			Does not require highly skilled employees to operate this solution	
		Medium	3	x		3				x		3	x		3
		Low	2	x		2	x		2	x		2	x		2
	Operational Impact	High	5		Operational impact would increase if a virus was detected and EDR had to kick into action		x	Scans can slow down devices so often need to be performed out of hours	5		Little or no operational impact			Little or no operational impact	
		Medium	3	x		3	x		3						
		Low	2	x		2	x		2	x		2	x		2
	Reliance on other tools	Yes	10		Reliant on AV controls however these would usually be built into EDR	5		No reliance on other cybersecurity solutions		x	Reliant on EDR (and some others) to report logs to it	10		No reliance on other cybersecurity solutions	
		No	0	x			x						x		
Total Available Score			50			35			22			32			11

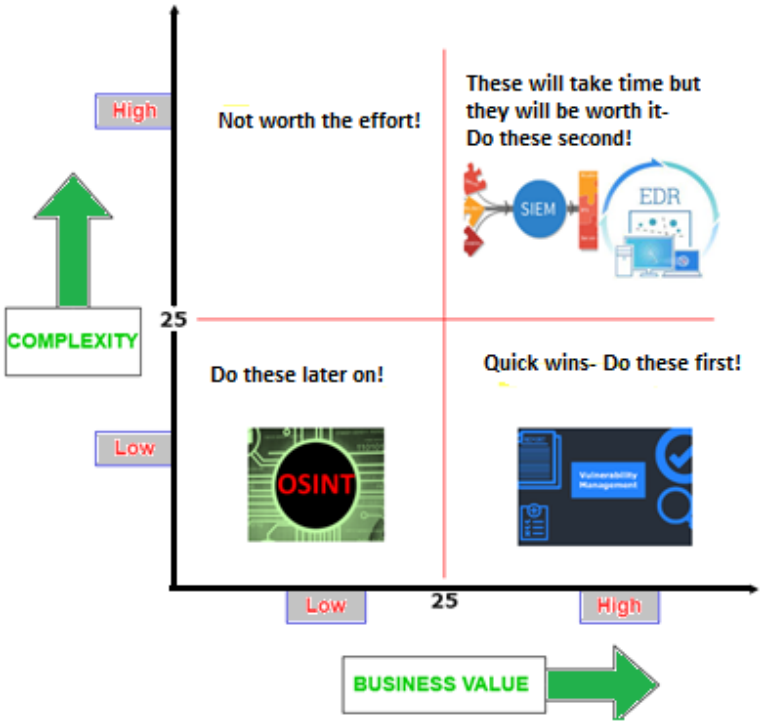
- ✓ EDR has come out on top with a score of 35 from a possible 50 in terms of the complexity of the control. It is a tool that requires some effort to implement and maintain and is also one which needs to be managed extremely carefully to avoid major incidents. Interestingly just 48% of survey participants understood fully the time/cost efforts to maintain this solution. This would suggest to me that people understand that it is quite a complex control.
- ✓ SIEM comes in second place with a score of 32 complexity. Again, this is something we would expect given the number of log sources that report into it and the potential different configurations for each, as well as the analysis level that it would provide on these logs. Over 44% of those surveyed did not understand the time/cost efforts to maintain this product. In my opinion this shows that although people view a SIEM as an important control, they are also aware that there is a level of complexity there which may not be conducive to a quick and easy implementation process.

- ✓ Vulnerability Management scores 22 which suggests that it may be an easier solution to roll out to an organisation. The fact that it does not rely on any other tools, and also that it is relatively easy to operate work as major selling factors for this cybersecurity solution. Having said that, less than half of those surveyed believed they understood the time/cost efforts
- ✓ OSINT scores just 11 out of 50 in this complexity. This is expected given the nature of the solution, it shows information available on the dark web so is not reliant on any other solutions, would not impact the business ops and is easily set-up and maintained.

These evaluation tables assessed these four cybersecurity solutions against the data points to give two different bottom line scores, one for Business Value and one for Complexity, which we can now use with our prioritisation matrix.

6.3 Prioritisation of Cybersecurity Solutions

When we plug all of these scores into our X Vs Y matrix we can see where each cybersecurity solution lies on the grid. The Business Value Vs Complexity model helps to prioritise what should be implemented first. What we want in this case is to focus on the cybersecurity solutions that deliver the highest value and require the least effort.



In this case we can see that Vulnerability Management resides in this bottom-right quadrant of the grid. So according to our metrics, **an organisation should prioritise Vulnerability Management in their roadmap**. This theory would make a lot of sense in the case of "Big Red Insurance" as VM scanning would uncover the main vulnerabilities so the IT Infrastructure and Security teams could focus on securing these users and devices without any delay.

According to my prioritisation matrix **EDR and SIEM should be implemented second and third respectively** as they both fall into the top right corner of the grid. This also means that they would be seen as having the highest value to an organisation but would be more complex and take longer to implement as a result. Often, this quadrant would be where the longer term projects would sit, so implementation may be started early knowing that they will take longer to complete, and other cybersecurity solutions may be started and finished before these larger projects are. These will take time but will be worth it. In this case it might be better to implement EDR before a SIEM so that the logs are ready to report to the SIEM once it has been implemented.

OSINT scored as low in Business Value but also low in Complexity. The recommendation for anything in this section would be to implement later on, perhaps when other solutions are already in place. It may score low in Business value but often the low complexity would weigh in its favour as this means it can be implemented quicker than any of the other controls and at a low cost, so could offer some pretty instant mitigation against cyber-risks while the organisation waits on other solutions to be onboarded.

These evaluation tables and prioritisation matrix helped me to successfully completed Objective#2 which was to score these four cybersecurity solutions against the data points to give two different bottom line scores, one for Business Value and one for Complexity. My online survey gave me something to measure these against, and the results show that the value of these solutions and how they should be prioritised are almost exactly the same as the perspective of my participants.

6.4 Critical Analysis and Implications

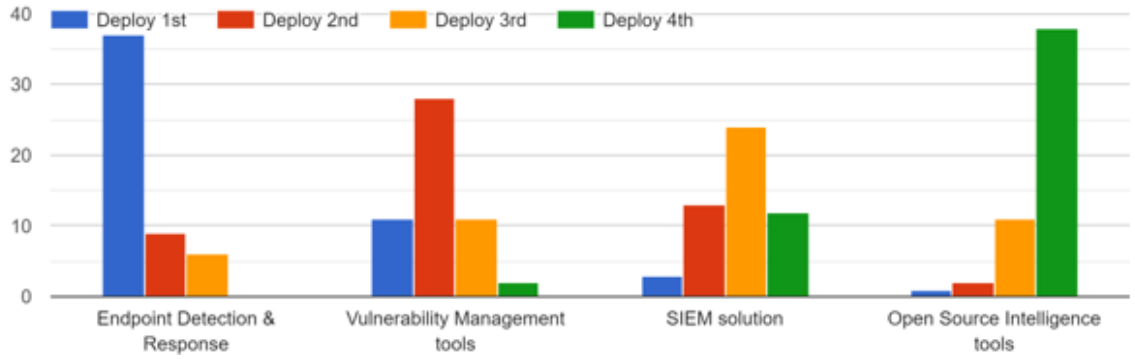
My research project findings would suggest that Vulnerability Management should be the first solution implemented, followed by EDR and then a SIEM solution as per table below.

Prioritisation (from my matrix)	
VM Scanning	1st
EDR	2nd
SIEM	3rd
OSINT	4th

Online Survey (what order would you deploy)	%
EDR	71
VM Scanning	53
SIEM	46
OSINT	73

71% of those surveyed believed that EDR should be the first cybersecurity implemented, followed by VM scanning and then a SIEM solution. These participants are likely to have voted for EDR assuming no other cybersecurity solution is in place, in which case I would agree with the survey results. On the other hand, if Anti-Virus was already in place within an organisation (as one would expect it to be) then I would side with my research project metrics and choose to implement VM scanning first in order to mitigate risks and for obvious regulatory obligations. See survey question below.

If you were the CISO (Chief Information Security Officer) of a company, in which order would you deploy the following cybersecurity controls?



My research project findings lined up exactly with my survey results in regard to OSINT. 73% of participants said it would be the fourth solution that they would implement out of the four.

Implications of this research project are that broadly speaking my results match up with the results of my online survey showing two outcomes, that my evaluations are accurate and well measured, and also that the perspective of these cybersecurity solutions is relatively accurate.

I hope that this research project can contribute towards understanding what cybersecurity solutions should be introduced to an organisation and when. CEO's or board members and students should be able to read the paper and find that it offers them some understanding on different areas of the project.

7. CONCLUSION AND FUTURE WORK

My conclusion from this research project is that there are a number of benefits both academically and within industry from this project. There can always be disagreements in organisations when trying to prioritise or de-prioritise one project or IT solution over another, so I would hope that my research project could be used to help this process, or even validate a decision one way or another.

It is quite obvious when comparing my findings with the results of the online survey, that there is a clear understanding about what the most valuable cybersecurity solutions are and how they should be prioritised. If I had known this at the start of the project I would probably have tried to change one or two of the solutions or even added a few more obscure ones to see how these fitted into the equation. The big plus-side of this however, is that this shows that my data points, my assessment table and my use of the Value V Complexity matrix, gave accurate outputs in terms of being able to assess differing cybersecurity solutions. Given more time here I would add in additional solutions such as Penetration testing tools, or Encryption tools to see how they score and also to see how they would be viewed by my survey participants.

Some limitations on the project was trying to get people to respond to the online survey. Although I achieved over my target of 50 participants I would have preferred to be able to collect a larger sample of data for accuracy purposes. I could also have done better with some of the survey questions, some of which I had created in the very early stages and by the time the project began to take shape, they seemed not as relevant anymore. The second half of the survey required some "knowledgeable" answers to proceed when some participants may not actually know the previous original answer. I should have given a "I don't know" answer to the last 5 questions. Unfortunately re-issuing the survey mid-way through the project was not an option for me as I was concerned about response numbers considering how slow the participants were to complete it the first time around. Another issue I ran into was that I found it difficult to to find out other companys spending on cybersecurity solutions and tools. It did help that in my role as Information Security Officer within my own company, I was able to get some of this information first hand but again I would have preferred a larger sample of data for accuracy purposes.

In regards to my data points, I would probably have revised these again and tried to add in some more. Although risk mitigation would provide a good overview of how well the cybersecurity solution would work, I would definitely still try to include "effectiveness" as a measurable data point next time and add it in to the scoring matrix for Business Value. In order to get a value for this I could maybe have taken top 10

vulnerabilities in 2021 based on CVSS score and made an analysis on how each of the cybersecurity solutions would fare in protecting our organisation against each of these vulnerabilities.

In terms of the evaluation of the four cybersecurity solutions, I believe that an organisation should have all four if they are serious about cybersecurity. I would certainly begin the process of implementing a SIEM early on as I feel this solution gives more benefit to an organisation than any other. However, in the case of "Big Red Insurance" I feel that quickly implementing an OSINT tool might provide some peace of mind to board members and stakeholders, so that they can get a quick overview of where the organisation is weak in terms of their infrastructure. EDR and Vulnerability Management would also be on my list as between all four solutions they would have a good coverage of the infrastructure of the organisation.

In my opinion this was a successful research project, I learned a lot throughout it, not only about cybersecurity solutions but also about research methods and the writing of reports. I felt that I succeeded in what I set out to do, achieved my objectives, and I hope that this research project will be of some use in the future, either academically or within industry.

8. ACKNOWLEDGEMENT

I would like to thank my supervisor Ross Spelman for all his patience, help and guidance throughout the research process. I also wish to express my gratitude towards Springboard and the National College of Ireland for giving me a chance to do this Masters in Cybersecurity. Thanks also to my manager, Stephen Parsons, for his help and support throughout the last 2 years. Finally, thanks to my wife Edel and my family for all their encouragement throughout the process. I would not have been able to do this without you.

Please find my Viva presentation here: https://www.youtube.com/watch?v=gmbbOCeyDS0

9. REFERENCES

Akhtar, S., Sheorey, P. A. & Bhattacharya, S., 2021. Cyber Security Solutions for Business in Financial Services: Challenges, Opportunities and the Way Forward. *International Journal of Business Intelligence Research,* June, 12(1), pp. 82-97.

Bhatt, S., Manadhata, P. K. & Zomlot, L., 2014. "The Operational Role of Security Information and Event Management Systems,". *IEEE Security & Privacy*, 12(5), pp. 35-41.

Checkpoint, 2022. *EDR vs Antivirus.* [Online]
Available at: https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-endpoint-detection-and-response/endpoint-detection-and-response-edr-benefits/edr-vs-antivirus/#:~:text=EDR%20vs%20Antivirus%20%2D%20What%27s%20The,wide%20range%20of%20potential%20threats.
[Accessed 05 July 2022].

Coresecurity, 2022. *Top 14 Vulnerability Scanners for Cybersecurity Professionals.* [Online]
Available at: https://www.coresecurity.com/blog/top-14-vulnerability-scanners-cybersecurity-professionals
[Accessed 05 July 2022].

Fakiha, B. S., 2020. Effectiveness of Security Incident Event Management (SIEM). *Journal of Forensic Medicine ,* 14(4).

IDA Ireland, 2022. *FInancial Services.* [Online]
Available at: https://www.idaireland.com/explore-your-sector/business-sectors/financialservices
[Accessed 11 July 2022].

Kostrecová, E. & Bínová, H., 2015. "Security Information and Event Management". *Paripex- Indian Journal of Research,* 4(2).

Mahajan, A., 2016. *Value vs Complexity: A Prioritization Tool.* [Online]
Available at: https://www.linkedin.com/pulse/value-vs-complexity-prioritization-tool-ankur-mahajan/
[Accessed 05 August 2022].

Petters, J., 2020. *What is SIEM? A Beginner's Guide.* [Online]
Available at: https://www.varonis.com/blog/what-is-siem
[Accessed 23 July 2022].

ProductPlan, 2022. *Value vs. Complexity.* [Online]
Available at: https://www.productplan.com/glossary/value-vs-complexity/#:~:text=Complexity%20Model%3F-,Value%20vs.,a%20quadrant%20and%20prioritized%20accordingly.
[Accessed 06 August 2022].

Rinaldi, A., 2020. *The Cost of Cybersecurity and How to Budget for it.* [Online]
Available at: https://www.mdsny.com/the-cost-of-cybersecurity-and-how-to-budget-for-it/
[Accessed 11 May 2022].

Samson, R., 2022. *Endpoint Detection And Response (EDR) Vs AntiVirus.* [Online]
Available at: https://www.clearnetwork.com/edr-vs-antivirus/
[Accessed 30 April 2022].
Sapphire, 2022. *What Does a SOC Analyst Do?.* [Online]
Available at: https://www.sapphire.net/cybersecurity/what-does-a-soc-analyst-do/
[Accessed 22 June 2022].
Security Boulevard, 2022. *Small Business Cybersecurity Budgets to Prevent Cyberattacks.* [Online]
Available at: https://securityboulevard.com/2022/06/small-business-cybersecurity-budgets-to-prevent-cyberattacks/
[Accessed 01 July 2022].
Sharpe, W., 2022. *Reconaissance: How Hackers Stake Out Your Business.* [Online]
Available at: https://www.corp-infotech.com/hacker-reconnaissance/
[Accessed 04 May 2022].
TechCentral.ie, 2018. *CEO attitudes to cyber security are all wrong.* [Online]
Available at: https://www.techcentral.ie/ceo-attitudes-cyber-security-wrong/
[Accessed 27 April 2022].
Trellix, 2022. *What Is Endpoint Detection and Response (EDR)?.* [Online]
Available at: https://www.trellix.com/en-us/security-awareness/endpoint/what-is-endpoint-detection-and-response.html
[Accessed 02 July 2022].
Voxco, 2022. *Research Methodology.* [Online]
Available at: https://www.voxco.com/blog/what-is-research-methodology/
[Accessed 03 July 2022].
Zeizel, A., 2022. *X-Force Research Update: Top 10 Cybersecurity Vulnerabilities of 2021.* [Online]
Available at: https://securityintelligence.com/posts/x-force-top-10-cybersecurity-vulnerabilities-2021/
[Accessed 10 July 2022].