Configuration Manual

MSc Research Project in Cyber Security
Computer and Security Software

Nathan Kelly
Student ID: x20211261

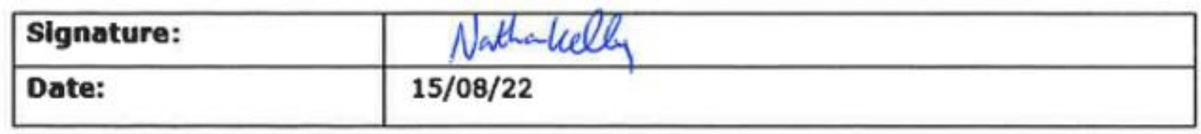
School of Computing
National College of Ireland

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:	Configuration Manual
Word Count:	4760
Page Count:	23

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:	Nathan Kelly
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):	

Configuration Manual

Nathan Kelly
X20211261

1 Introduction

My configuration manual accompanies the main research paper style report which together make up my research project.

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

1.1 Motivation of the Document

This configuration manual describes in more detail some of the work which went into researching this topic. This document was created alongside the research project paper and offers further information, and a more in-depth analysis, on many areas of the research project. including further details on:

- the chosen cybersecurity solutions
- the data points which were used to score each of these
- explanations on the scoring
- the online survey from which data was extracted

1.2 Configuration Manual Structure

Section 2 of the document outlines some of the extended research which took place involving multiple other cybersecurity solutions before I decided on the final four solutions for the research project. This section also names and explains what these four cybersecurity solutions do and some extended commentary on them.

Section 3 discusses the various data points used to compare the cybersecurity solutions and discusses these in further details. Here I try to expand on the data point a bit further and also explain why each of the data points was chosen to evaluate these cybersecurity solutions.

Section 4 explains the evaluations that I have given to each of the cybersecurity solutions versus each data point. I have tried to explain to the reader a bit further why this score was decided upon. I have also included a larger scale version of the Business Value and Complexity Evaluation tables which may be easier to read than the ones in the research project report.

Finally, Section 5 shows full details of my online survey, with screenshots displaying every question and subsequent answer. I also provide some commentary on each question and answer given.

2 Cybersecurity solutions

Initially I was unsure which cybersecurity solutions to focus on as there are so many being used in industries today. Many of these tools or solutions cover different areas of cybersecurity so it was important to try and choose cybersecurity solutions which were independent of each other and with as little crossover as possible.

Some of the different types or categories of cybersecurity tools investigated were:

- ✓ Encryption tools
- ✓ Anti-Virus tools
- ✓ Network Security Monitoring tools
- ✓ Network Defence Wireless tools
- ✓ Public Key Infrastructure (PKI) Services
- ✓ Packet Sniffers
- ✓ Firewall
- ✓ Web Vulnerability Scanning tools
- ✓ Managed Detection Services
- ✓ Penetration Testing services

(Software Testing Help, 2022)

After much research and thought I decided to choose four different cybersecurity solutions which I felt were particularly relevant to modern businesses and in particular, Irish Financial Service organisations. These four solutions are listed below along with a more detailed explanation of what they do.

2.1 Endpoint Detection and Response (EDR)

“Endpoint detection and response (EDR) is a system to gather and analyse security threat-related information from computer workstations and other endpoints, with the goal of finding security breaches as they happen and facilitating a quick response to discovered or potential threats. The term "endpoint detection and response" only describes the overall capabilities of a tool set. Therefore, the details and capabilities of an EDR system can vary greatly depending on the implementation.” (Wright, 2022)

EDR solutions may include anti-virus so are viewed as more evolved versions of EDR. “Anti-Virus (AV) provides the ability to detect and respond to malware on an infected computer using a variety of different techniques. EDR incorporates AV and other endpoint security functionality providing more fully featured protection against a wide range of potential threats.” (Checkpoint, 2022)

2.2 Vulnerability Management Scanning

“A vulnerability scanner is a computer program designed to assess computers, networks or applications for known weaknesses. These scanners are used to discover the weaknesses of a given system. They are utilized in the identification and detection of vulnerabilities arising from misconfigurations or flawed programming within a network-based asset such as a firewall, router, web server, application server, etc. Modern vulnerability scanners allow for both authenticated and unauthenticated scans.” (Wikipedia, 2022) It is an automated process which can proactively identify security vulnerabilities with a network. These scans can also help to predict how effective countermeasures are in case of a threat or attack. (RedLegg, 2019)

2.3 Security Information Event Management (SIEM) solution

A SIEM solution provides a real time analysis of security alerts which are generated as a result of logs being sent from all devices on a netowrk including applications and network hardware. “Security information and event management (SIEM) is an approach to security management that combines SIM (security information management) and SEM (security event management) functions into one security management system. The underlying principles of every SIEM system is to aggregate relevant data from multiple sources, identify deviations from the norm and take appropriate action.

For example, when a potential issue is detected, a SIEM system might log additional information, generate an alert and instruct other security controls to stop an activity's progress. At the most basic level, a SIEM system can be rules-based or employ a statistical correlation engine to establish relationships between event log entries. Advanced SIEM systems have evolved to include user and entity behavior analytics and security orchestration, automation and response.” (Rosencrance, 2020)

2.4 Open-Source Intelligence Tools (OSINT)

As outlined in the research project paper, these OSINT tools offer a view of what a hacker can see on the dark web and show the sort of information that a bad actor would try to discover as part of their reconaissance on an organisation. OSINT should offer continuous objective visibility of an organisations entire internet risk surface, spanning managed IT, and parts of a network which may have been forgotten. It allows the organisation to see the intimate details of every system, the detailed IT profile and security configuration, showing the data types at risk in every system. (RiskRecon, 2022)

3 Data points

In order to be able to compare the cybersecurity solutions we needed to come up with a number of data points to score each solution against.

Below are the data points used to evaluate the various solutions with an extended explanation for their inclusion in this research project:

- **Cost to Implement:** How much will it cost to implement this control into the organisation? As we have outlined in the main report, money is everything in modern-day business. So, the cost of implementing a tool can often be the biggest factor in the decision on whether to implement it or not within an organisation. This is a key data point to be considered in any comparative analysis or prioritisation.

- **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. This is another data point focussed around money, but an equally important one. A chosen cybersecurity solution may be inexpensive to implement but if it is going to cost a lot to maintain every year then this should be considered.

- **Reporting Ability:** Does the solution have the ability to provide clear and accurate reports? Often the only thing that a CEO or board will be able to judge a cybersecurity solution on is a one-page report. This may seem harsh, but unless the solution can summarise and “take credit for” all of the good work that it is doing for an organisation then this could go unnoticed within a board room. Hence reporting is key, not only from a board level, but so that the information security analysts can quickly and easily pinpoint where the vulnerability lies and what can be done to address it.

- **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? Risk mitigation is another term that I could have used for this. This could be linked to Inherent Vs Residual risk. “Inherent Risk is typically defined as the level of risk in place in order to achieve an entity's objectives and before actions are taken to alter the risk's impact or likelihood. Residual Risk is the remaining level of risk following the development and implementation of the entity's response.” (Tennessee State Government, 2022)

- **Regulatory Obligations:** Would the organisation be obliged by CBI rules and regulations to have certain cybersecurity solutions in place? The CBI strictly governs

Irish Financial Services companies, and there are requirements or regulations in place for these organisations to be aware of their vulnerabilities, and have documented plans in place to address them. This is another key data point that needs to be considered.

- **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? IT Teams are busy, so this is always an important consideration when looking to onboard any new solutions or controls.

- **Effort to Maintain:** How many days will the organisation need to spend weekly/monthly to maintain the upkeep of this? Will this solution require an additional member of staff to maintain it? Or can this be worked into normal BAU activities?

- **Difficulty to Operate:** How easy is the solution to operate? What is the availability of talent to operate this? This is a more simplistic data point, but an important one nonetheless. If a cybersecurity solution is onboarded but there are no skilled employees available to manage it, then it is not much of much benefit to the business.

- **Operational Impact:** Does the solution slow down machines or impact users in any way? An example where a cybersecurity solution might slow down a system would be a Nessus scan on a particular server, these can be "noisy scans" meaning that they affect the operations of the server. This could result in users seeing their applications slowing down or freezing. Ideally an organisation would prefer if the solution did not affect the productivity of their users or have any other operational impact.

- **Reliance on other tools:** How reliant is this on other cybersecurity solutions or tools which may or may not already exist in the organisation? It isn't much use onboarding a cybersecurity solution and then realising it doesn't work without a plethora of other solutions. Hence this should be considered so that the solution is not implemented and then deemed not fit for use.

4 Scoring, Formula and Metrics

Here I provide some further details on the scores and the reasons for the scores. Each score is from a maximum of 10.

4.1 Scoring for each Data Point related to Business Value

Cost to Implement:

- ✓ **EDR Score:** 5
  Reason for score: 20 days to roll out at a typical contractor rate of €1000 per day (from a company like Sureskills) means the solution costs less than €25,000. (Fitzpatrick, 2018)

- ✓ **Vulnerability Management Score**: 7
  Reason for score: If an appliance scanner was used here then this would cost less than €10,000 to implement.

- ✓ **SIEM score:** 3
  Reason for score: Getting logs set up to go from 50 servers, some of which may be Windows Exchange servers, or Linux servers would represent a high level of work. We also need logs reporting from Anti-Virus or EDR, any Multi-Factor Authentication (MFA) in place, or firewalls just to name a few. As a result of this the implementation cost would be over €25,000 but less than €50,000.

- ✓ **Open-Source Intelligence Tool score:** 10
  Reason for score: The annual licence cost of a typical OSINT solution such as Black Kite or RiskRecon would be between €1500-€2400 which is below €2500 meaning the max score is achieved here.

Cost to Maintain:

- ✓ **EDR Score:** 5
  Reason for score: Based on 200 endpoints costing €57 per endpoint this would come to just under €12,000. This €57 quote came from Checkpoint for Checkpoint Sandblast EDR.

- ✓ **Vulnerability Management Score:** 7
  Reason for score: Based on 200 endpoints costing €35 per endpoint this would come to €7,000. This quote came from a 3rd party provider who provide VM scanning options and use Qualys as their scanning device.

- ✓ **SIEM score:** 3
  Reason for score: This score is based off EPS (events per second) However as a guideline this number of endpoints (device and servers) would produce a sizeable number of logs likely to cost the organisation up to €50,000 per annum.

- ✓ **Open-Source Intelligence Tool score:** 10
  Reason for score: For most OSINT products, this is a once off licence fee of between €1500-€2400.

Reporting ability:

- ✓ **EDR Score:** 10

  Reason for score: EDR would go into great detail when reporting on anything suspicious found on a device. This could include forensic analysis as well as recommended mitigations.

- ✓ **Vulnerability Management Score:** 10
  Reason for score: Reporting would usually contain thousands of different vulnerabilities which would be categorised from a 1-5 where 1 is insignificant and 5 would be major. These large lists of vulnerabilities would also usually contain remediations and recommendations on how to close them out.

- ✓ **SIEM score:** 10
  Reason for score: The SIEM by its very nature would go into very specific details of any anomaly detected and report on this through the logs it receives. It would also provide recommendations on steps towards remediating the vulnerability.

- ✓ **Open-Source Intelligence Tool score:** 1
  Reason for score: OSINT reports on what can be seen on the dark web. This may be simplistic details like a password, or an open port but would typically not go any further than that.

Risk of not having the tool in place:

- ✓ **EDR Score:** 10
  Reason for score: There would be a high risk of not having EDR in an organisation. EDR offers so much detail on an individual endpoint level so to not have this would mean there are large gaps in knowledge in terms of what malicious files, or software, could potentially be present on any endpoint.

- ✓ **Vulnerability Management Score:** 5

Reason for score: Vulnerability Management is still something that a lot of organisations would see as a luxury. However, it has so much to offer and can often identify vulnerabilities that other cybersecurity solutions would not have scope of. In my opinion, while the risk may not be high of not having this in place, it would still be substantial so a score of 5 is appropriate here.

- ✓ **SIEM score:** 8
  Reason for score: In my opinion there would be a high risk of not having this tool in place especially given the surface area that it covers. Every device that produces logs can be set up to report to a SIEM and that gives the organisation a great overview of what is happening on their network. While the risk may not be very high, I would still rate it as high and a score of 8.

- ✓ **Open-Source Intelligence Tool score:** 0
  Reason for score: No risk of not having this tool in especially if other cybersecurity solutions are already in place.

Regulatory obligations:

- ✓ **EDR Score:** 10
  Reason for score: EDR is something that is required by regulations. The regulations state that each endpoint must be monitored, and while anti-virus might also tick this box, EDR gives the extra add-ons of taking active actions if malicious software or files are discovered, which is also a CBI requirement.

- ✓ **Vulnerability Management Score:** 0
  Reason for score: The CBI regulations state that a company needs to be aware of their vulnerabilities, but there are a number of cybersecurity solutions which would satisfy this requirement, it does not necessarily have to be a VM scanner. So as far as regulatory obligations go this scores 0.

- ✓ **SIEM score:** 10
  Reason for score: While the CBI regulations do not specifically mention a requirement for a SIEM in place, it does request that logs are collected and analysed in a central location, which is exactly what the SIEM does. There are no other solutions out there which can manage this to the requirements of the CBI apart from a SIEM. Hence the high scoring here.

- ✓ **Open-Source Intelligence Tool score:** 0
  Reason for score: No regulatory obligations in place for a financial services company to have OSINT in place.

4.2 Scoring for each Data Point related to Complexity

Effort to Implement:

- ✓ **EDR Score:** 10
  Reason for score: EDR can be difficult to roll out across a network. For example, a file server would be relatively straightforward to roll this out to, however an Exchange server would need to be specifically configured otherwise it could cause the server to crash. So, the real complexity of implementing this solution is trying to follow best practice for each server type as recommended by vendors. This explains the high complexity score here.

- ✓ **Vulnerability Management Score:** 5
  Reason for score: Certainly not as difficult to roll out as EDR but there is still a level of difficulty in rolling this out across a network. There are two options to do this, one would be an agent rolled out to all endpoints, the other would be an appliance scanner which is set up with visibility of all endpoints so it can scan them. The latter is the easier option but still requires time and effort. It would be expected that this would be rolled out to 200 endpoints in 10 days or less.

- ✓ **SIEM score:** 10
  Reason for score: Implementing a SIEM solution into any organisation is an onerous task. Different servers need to be onboarded in different ways so that the logs they are producing can be parsed correctly and accurately. This can mean onboarding servers one-by-one and testing to ensure the logs are coming through. This is time-consuming but should do done within 25 days.

- ✓ **Open-Source Intelligence Tool score:** 0
  Reason for score: The effort to implement OSINT is little or none. Once the company and domain names are known they can use their scanning tools to do the rest. Typically, this would only take a couple of hours to implement fully.

Effort to Maintain:

- ✓ **EDR Score:** 5

  Reason for score: Once this solution is in place there is little maintenance required on it. From speaking to my own company's infrastructure team, they advised they would not spend more than 1 hour per week on maintaining this. The very nature of EDR, using Checkpoint Sandblast as a specific example, is that it would scan and assess all files before being downloaded and block those that it saw as potentially malicious. On occasion some of these could be false positives and may need to be whitelisted. Aside from that the product does not require a large effort to maintain.

- ✓ **Vulnerability Management Score:** 5
  Reason for score: If this solution is implemented correctly at onboarding, then there should be little effort to maintain it. Newly built devices would need to be added into scans, and old retired devices would need to be removed, but otherwise this should be a smooth process and not take more than 5 hours per month.

- ✓ **SIEM score:** 5
  Reason for score: The main cause for maintenance on a SIEM is log sources which may stop reporting from time to time. These would usually occur due to an OS or patching update but aside from that there should be little maintenance.

- ✓ **Open-Source Intelligence Tool score:** 2
  Reason for score: Occasionally false positives may show up in results and need to be acknowledged or marked accordingly. Some calibration of the results can be required but again this is negligible. 2 hours per month should cover all maintenance for this solution.

<u>Difficulty to Operate:</u>

- ✓ **EDR Score:** 10
  Reason for score: EDR is a complex cybersecurity solution and would require training to be able to operate correctly, otherwise mistakes can be made which could potentially cause downtime.

- ✓ **Vulnerability Management Score:** 2
  Reason for score: Once VM scanning has been implemented it should be as simple as the click of a button to perform a scan on the network. Hence a low score here for this data point.

- ✓ **SIEM score:** 5
  Reason for score: A SIEM can take some time to get used to and although it has a lot in there, it is not overly technical and does not require a high level of expertise to operate, hence the medium score for this.

- ✓ **Open-Source Intelligence Tool score:** 5
  Reason for score: OSINT tools are generally very manageable. The vulnerabilities are detected and displayed on an online dashboard. No expert training or technical expertise is required to be able to run them, though it may take some time to get up to speed on the portal. A medium score has been given for this reason.

Operational Impact:

- ✓ **EDR Score:** 5
  Reason for score: Generally, EDR would not have much of an operational impact, but on occasion if it did detect a potentially malicious file on a server or endpoint it could take some time analysing it and sandboxing it which could result in a slowdown of the system processes. Having said that, this would be rare, but enough to warrant a medium score here.

- ✓ **Vulnerability Management Score:** 10
  Reason for score: VM scans would often slow down devices, especially something like a file server so it would be recommended to perform these scans out of business hours. However, when running this would have a high operational impact.

- ✓ **SIEM score:** 2
  Reason for score: The SIEM is merely collecting the logs from each device so operational impact would be negligible.

- ✓ **Open-Source Intelligence Tool score:** 2
  Reason for score: Another tool with little or no operational impact hence the low scoring rating.

Reliance on other tools:

- ✓ **EDR Score:** 5
  Reason for score: EDR would be reliant on Anti-Virus normally but given that this would usually be built into an EDR product I am giving this a score of 5, which is a medium level of reliance and halfway marker between the high and low scoring.

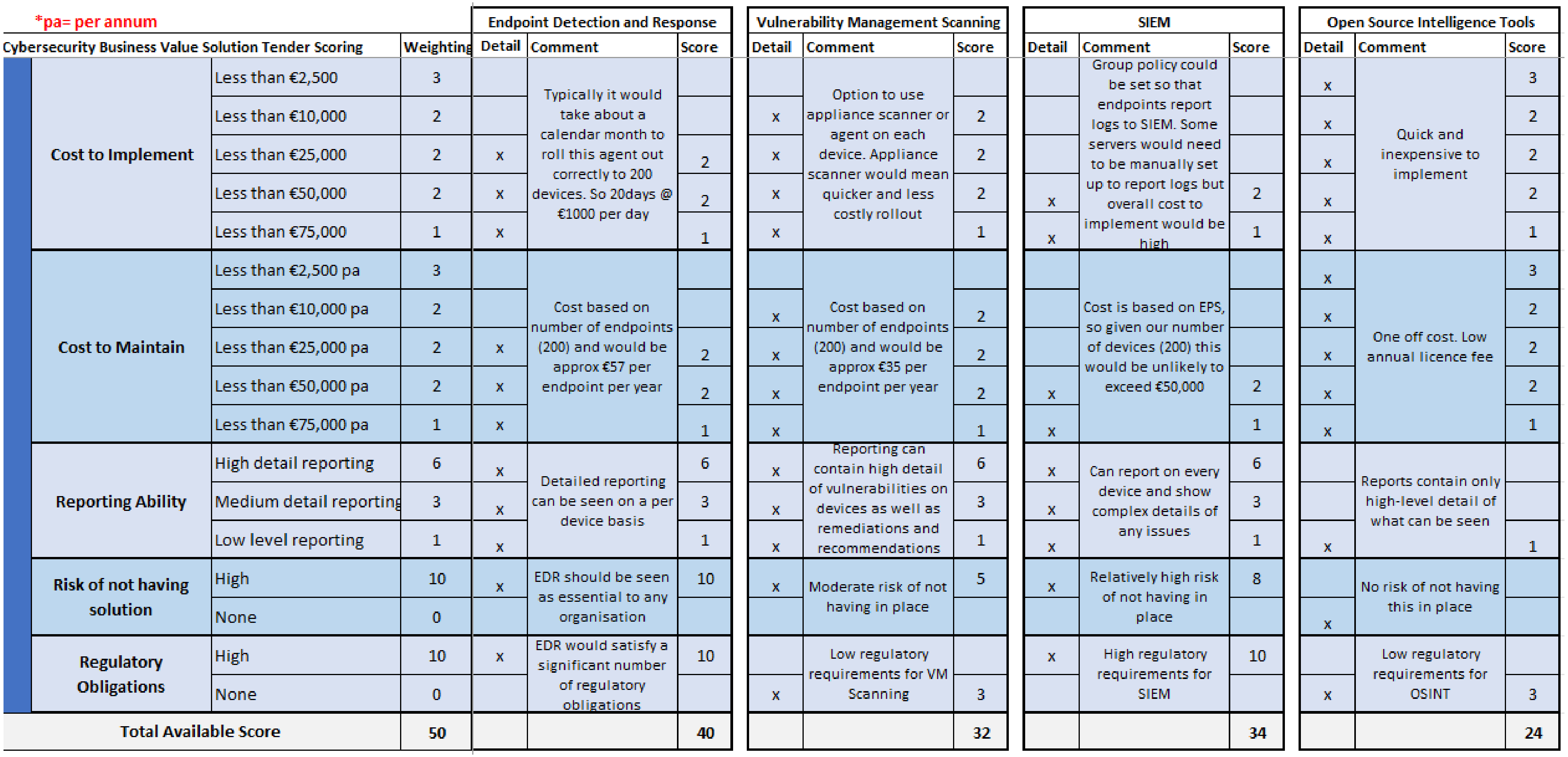
- ✓ **Vulnerability Management Score:** 0
  Reason for score: No reliance on other cybersecurity solutions.

- ✓ **SIEM score:** 10
  Reason for score: The SIEM relies on logs from all devices on the network. That would include other cybersecurity solutions like AV or EDR, so there is a high reliance here hence the scoring.

- ✓ **Open-Source Intelligence Tool score:** 0
  Reason for score: No reliance on other cybersecurity solutions.

4.3 Business Value of Cybersecurity Solutions Evaluation table

I have included this evaluation table in the configuration manual in a larger text format just so it is easier to read as the text was quite small in the research project report.

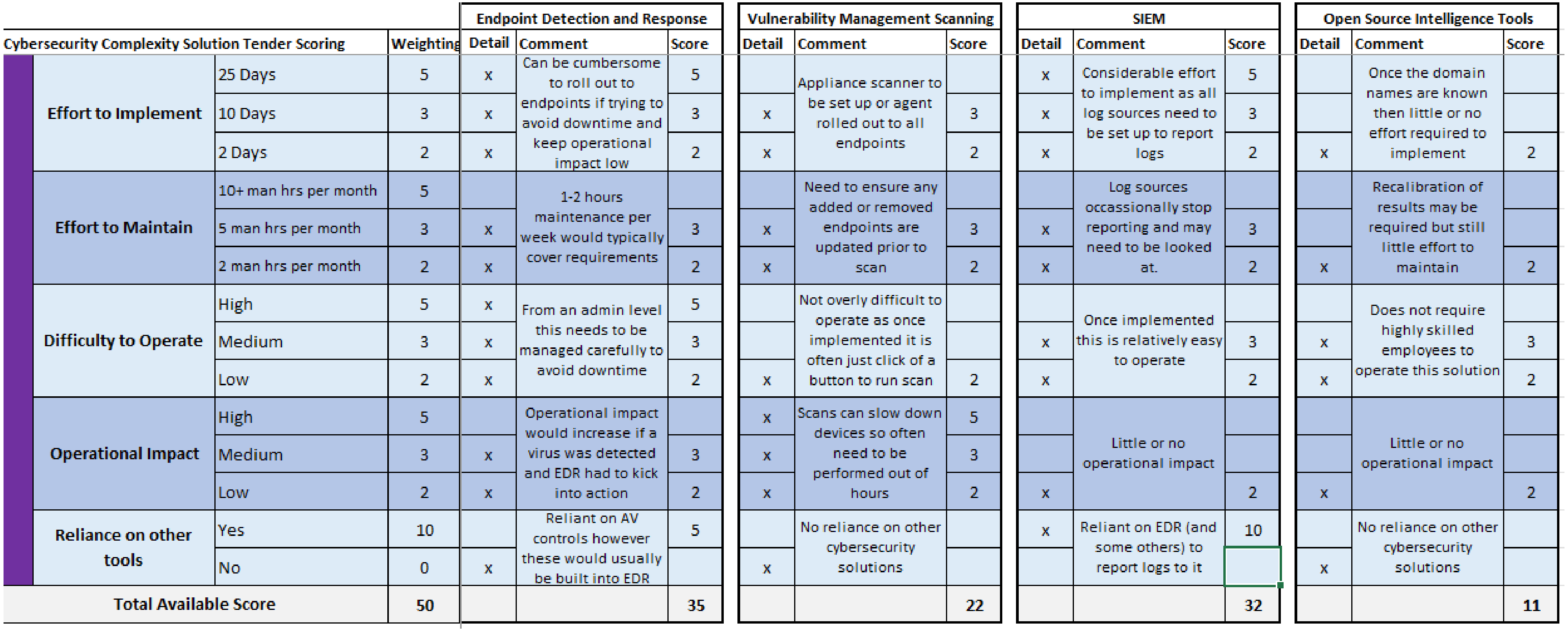


*pa= per annum

			Endpoint Detection and Response			Vulnerability Management Scanning			SIEM			Open Source Intelligence Tools		
Cybersecurity Business Value Solution Tender Scoring		Weighting	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

4.4 Complexity of Cybersecurity Solutions Evaluation table

I have included this evaluation table in the configuration manual in a larger text format just so it is easier to read as the text was quite small in the research project report.



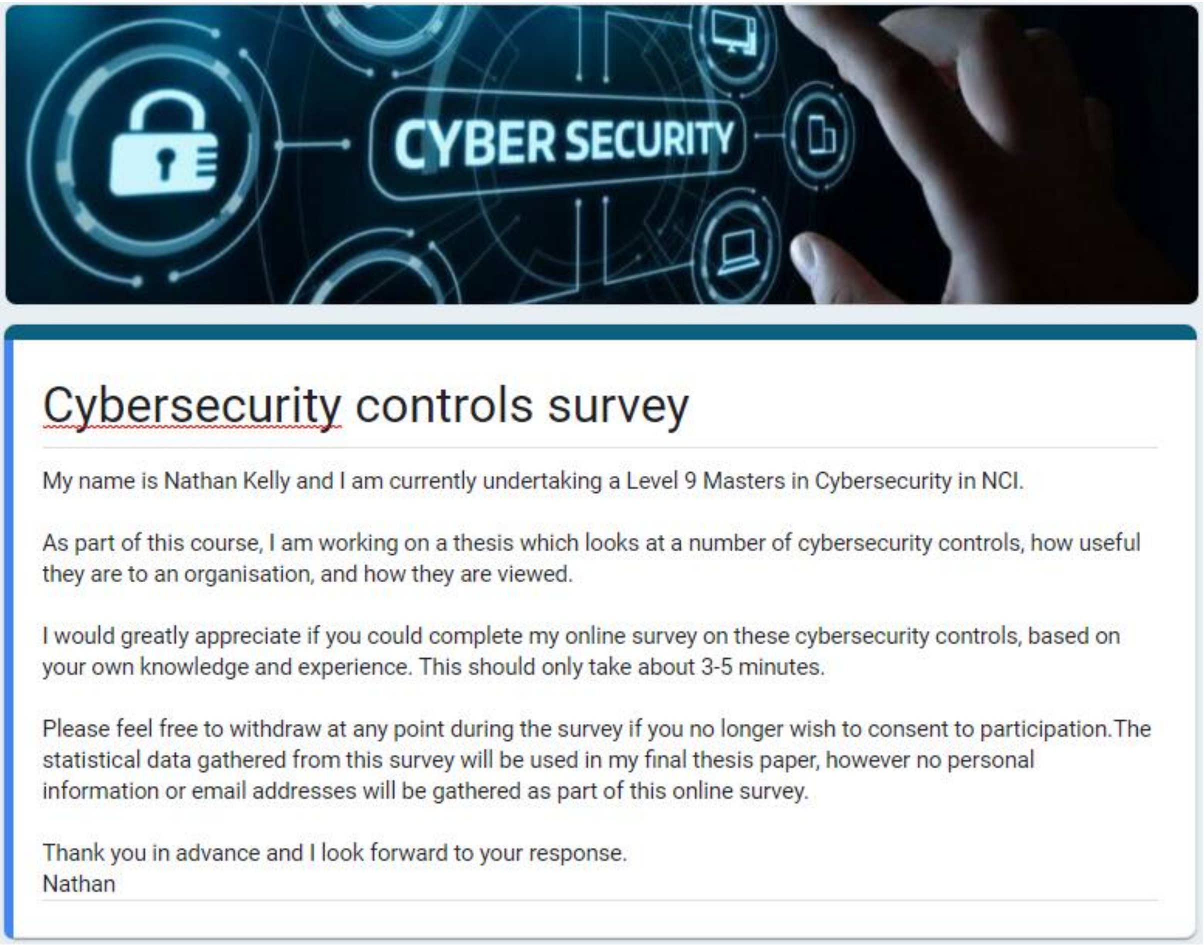
			Endpoint Detection and Response			Vulnerability Management Scanning			SIEM			Open Source Intelligence Tools		
Cybersecurity Complexity Solution Tender Scoring		Weighting	Detail	Comment	Score	Detail	Comment	Score	Detail	Comment	Score	Detail	Comment	Score
Effort to Implement	25 Days	5	x	Can be cumbersome 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

5 Survey

The main purpose of my survey was to collect my own data to help provide a view of how each of these cybersecurity solutions are viewed across different industries.

The survey was created and shared on Linkedin as well as with some present and former work colleagues. The main respondents were those involved in the IT or Cybersecurity area within their companies. However, there were also responses from non-IT based participants. Business Professionals, Change Management Professionals, Audit and Compliance Professionals, Graduates, Students, and Interns also gave their feedback within the survey.

The survey contained 18 questions which could be answered in various forms like multiple choice, dropdowns or check boxes. Below are my survey questions and responses along with some commentary.



Cybersecurity controls survey

My name is Nathan Kelly and I am currently undertaking a Level 9 Masters in Cybersecurity in NCI.

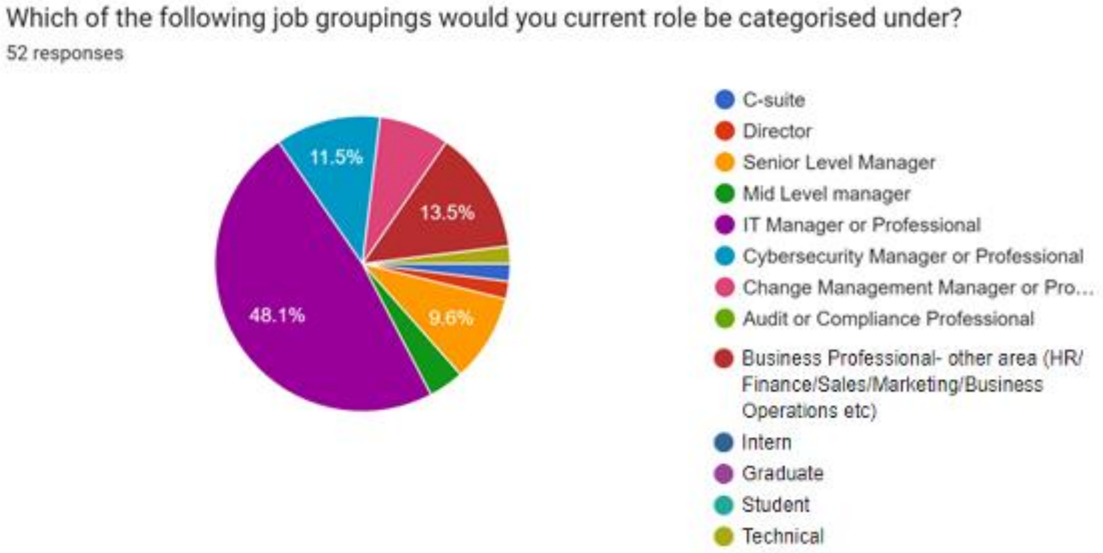
As part of this course, I am working on a thesis which looks at a number of cybersecurity controls, how useful they are to an organisation, and how they are viewed.

I would greatly appreciate if you could complete my online survey on these cybersecurity controls, based on your own knowledge and experience. This should only take about 3-5 minutes.

Please feel free to withdraw at any point during the survey if you no longer wish to consent to participation.The statistical data gathered from this survey will be used in my final thesis paper, however no personal information or email addresses will be gathered as part of this online survey.

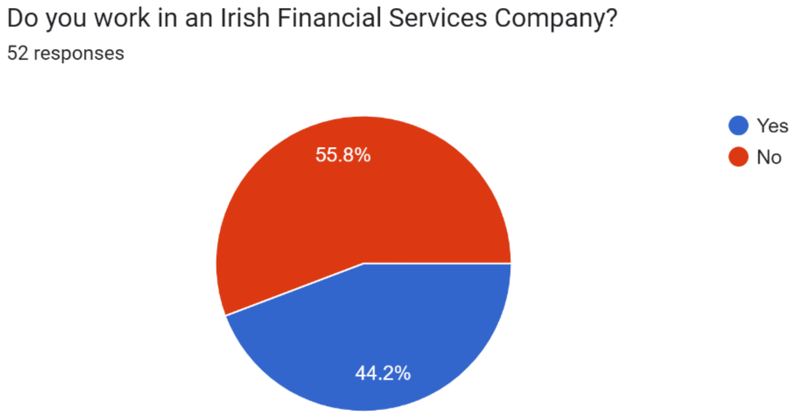
Thank you in advance and I look forward to your response.
Nathan

Question 1 asks about the current occupational role of the participant.



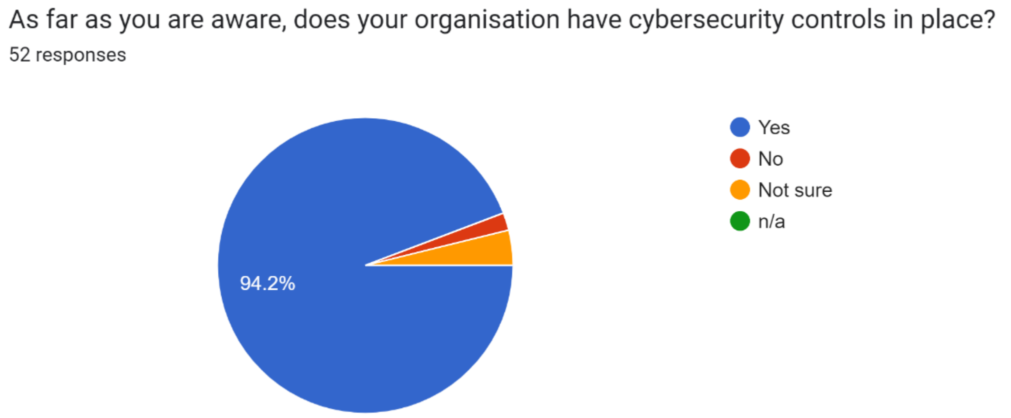
- Almost 60% of the participants are involved in IT or Cybersecurity roles suggesting that this is quite an educated group within this field.
- 8 of the 52 responses are senior managers, directors or C-suite who are the people within an organisation who may be involved in making the decisions over what cybersecurity solutions to implement.

Question 2 asks the participants if they work in an Irish Financial Services organisation.



- Almost half of the participants work in the financial services industry, the same area of business as our fictional company "Big Red Insurance." This is useful as it means my results and the answers given in survey are from somewhat "like for like" companies.

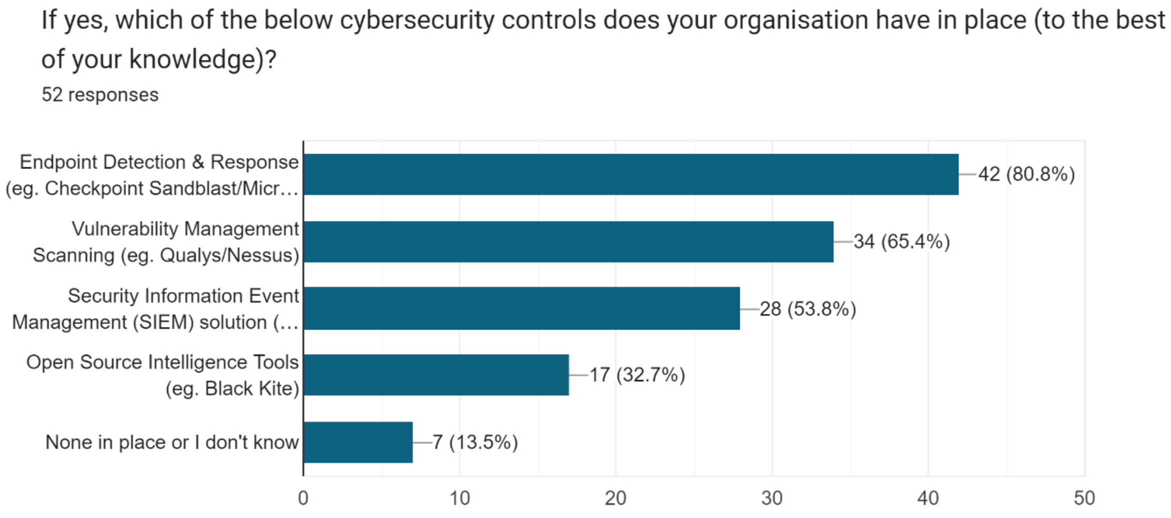
Question 3 queries if the participants are aware of any cybersecurity controls within their workplace.


As far as you are aware, does your organisation have cybersecurity controls in place?

52 responses

- Interestingly, only 2 respondents out of 52 were unaware of this while 1 further person said no. This shows us how big a part of business cybersecurity has become that people are aware of this.

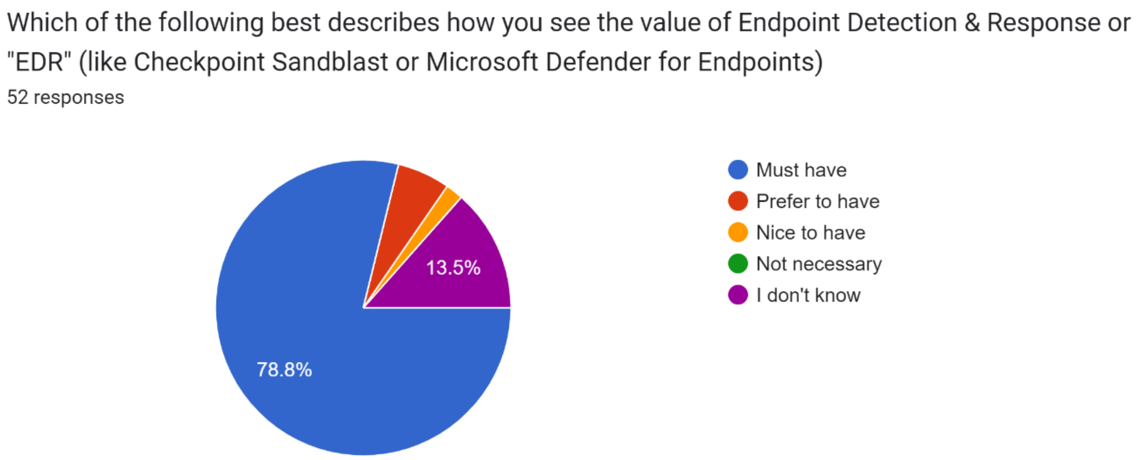
Question 4 asks to the best of their knowledge, what cybersecurity controls are in place within their workplace.


If yes, which of the below cybersecurity controls does your organisation have in place (to the best of your knowledge)?

52 responses

- EDR is top of this list, as we might expect it to be. OSINT is bottom, possibly as it is the least well-known out of all of these, or possibly because it is in the least number of organisations.
- Vulnerability Mgmt scanning comes in second place- with two thirds of participants saying it was in their organisation, ahead of a SIEM solution which 54% of users clicking to say that their organisation used this as a cybersecurity control.

Question 5 asks about the participants view on EDR and asks it to categorise its importance into one of five groups.

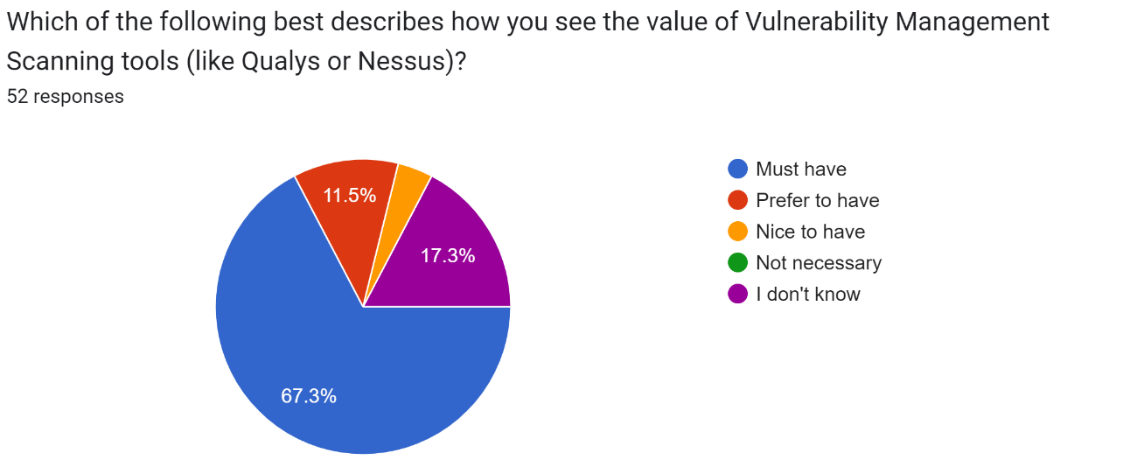


Which of the following best describes how you see the value of Endpoint Detection & Response or "EDR" (like Checkpoint Sandblast or Microsoft Defender for Endpoints)

52 responses

- Almost 80% of participants viewed EDR as a "must-have."

Question 6 asks about the participants view on Vulnerability Management scanning and asks it to categorise its importance into one of five groups.

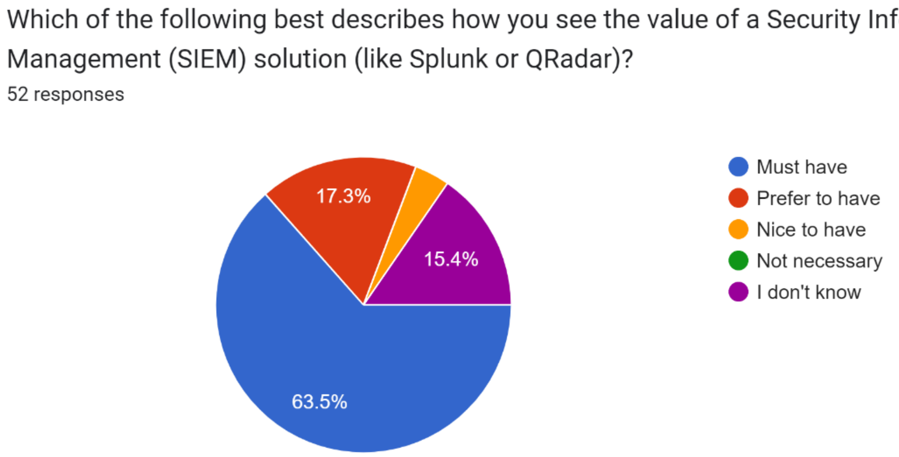


Which of the following best describes how you see the value of Vulnerability Management Scanning tools (like Qualys or Nessus)?

52 responses

- Over two thirds of participants viewed Vulnerability Management scanning as a "must-have."

Question 7 asks about the participants view on a SIEM and asks it to categorise its importance into one of five groups.

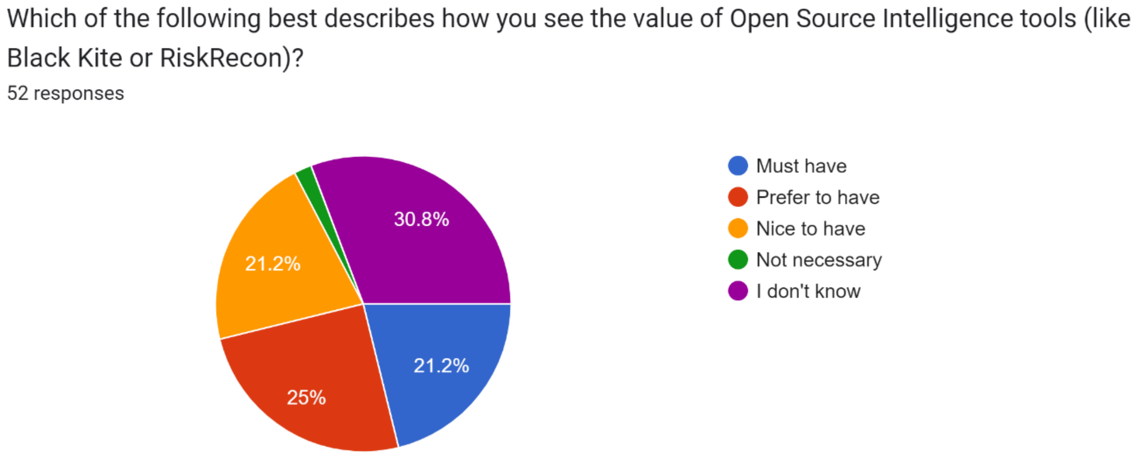


Which of the following best describes how you see the value of a Security Information Event Management (SIEM) solution (like Splunk or QRadar)?

52 responses

- 63.5% of participants viewed SIEM as a “must-have.”

Question 8 asks about the participants view on OSINT and asks it to categorise its importance into one of five groups.

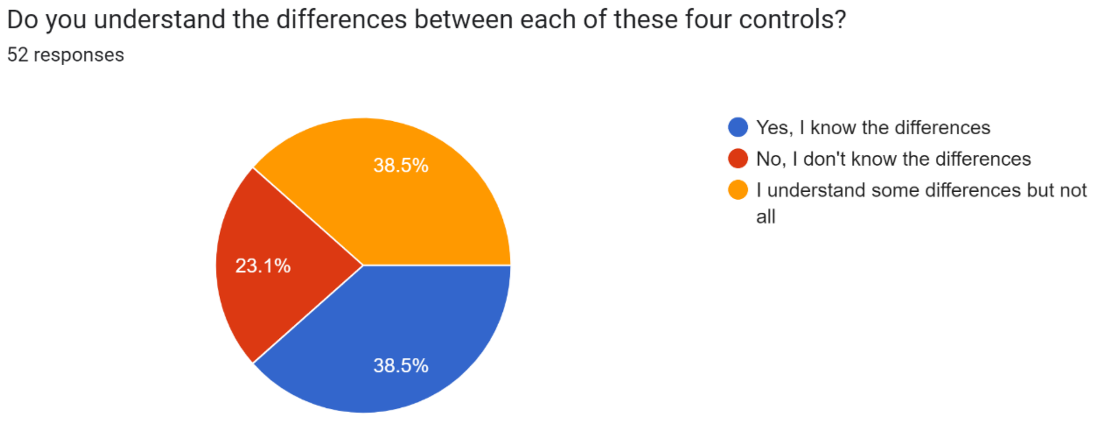


Which of the following best describes how you see the value of Open Source Intelligence tools (like Black Kite or RiskRecon)?

52 responses

- 21% saw OSINT as a “must-have,” but another 31% were not sure about this one.

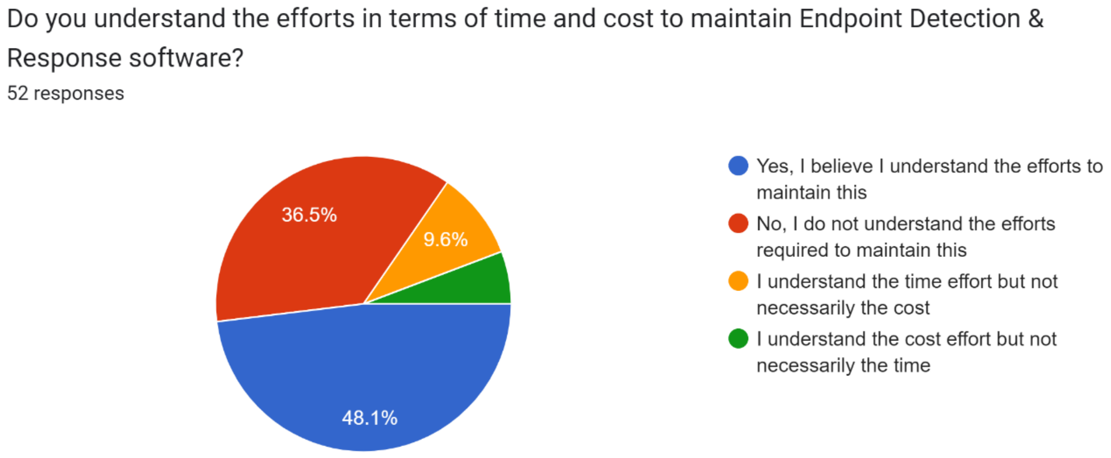
Question 9 then asks if the participant knows the differences between all of these four cybersecurity controls.


Do you understand the differences between each of these four controls?

52 responses

- 20 of the 52 participants were confident that they understood the differences and another 20 believed that they understood some but not all differences. This again demonstrates that the majority of the audience here has or think that they have a reasonable understanding of these cybersecurity solutions.

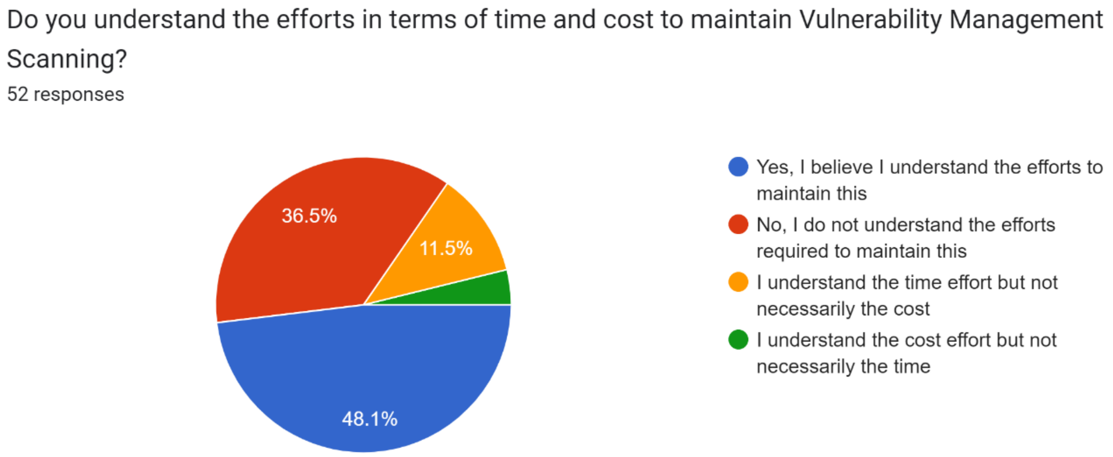
Question 10 queries the participant on whether they understand the efforts in terms of time and cost to maintain EDR.


Do you understand the efforts in terms of time and cost to maintain Endpoint Detection & Response software?

52 responses

- Nearly half (48%) of the participants understood the efforts to maintain this control, another 16% understood one or the other.
- 36.5% said they did not understand the efforts to maintain this. This is where my metrics may be able to help such participants.

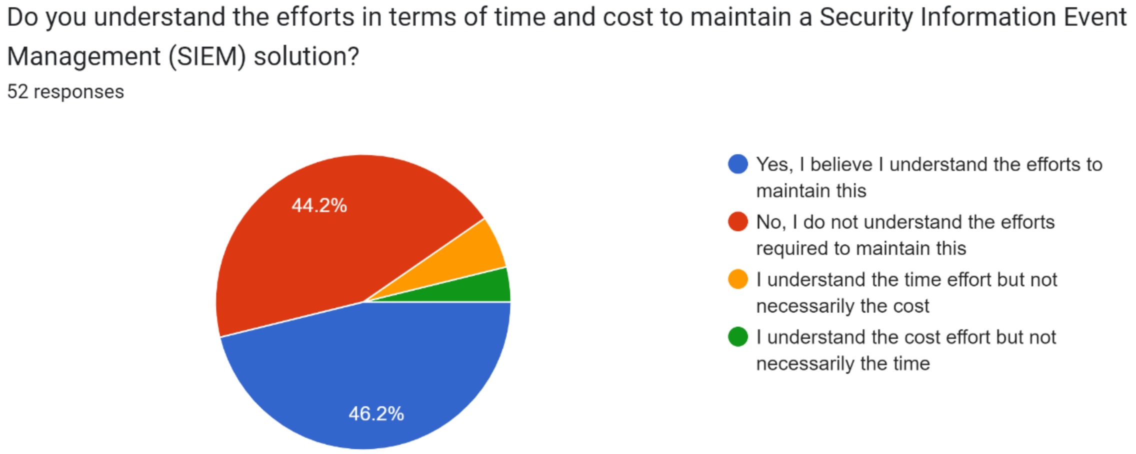
Question 11 queries the participant on whether they understand the efforts in terms of time and cost to maintain Vulnerability Management Scanning.


Do you understand the efforts in terms of time and cost to maintain Vulnerability Management Scanning?

52 responses

- Again, just under half of the participants understood the efforts to maintain this control and another 16% understood one or the other.
- 36.5% said they did not understand the efforts to maintain this.

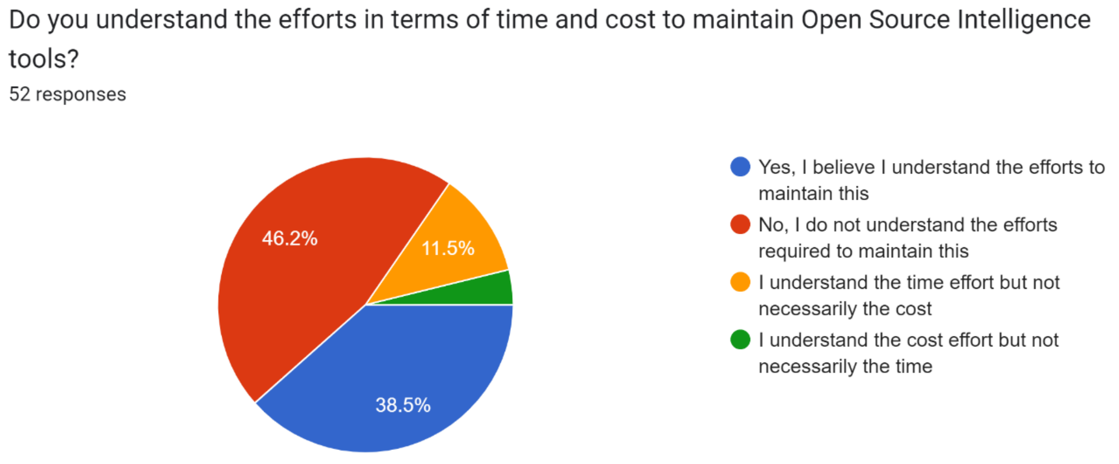
Question 12 queries the participant on whether they understand the efforts in terms of time and cost to maintain a Security Information Event Management (SIEM) solution.


Do you understand the efforts in terms of time and cost to maintain a Security Information Event Management (SIEM) solution?

52 responses

- 46% of participants understood the efforts to maintain this Vs 44% of participants who did not. This shows there is a level of uncertainty here.

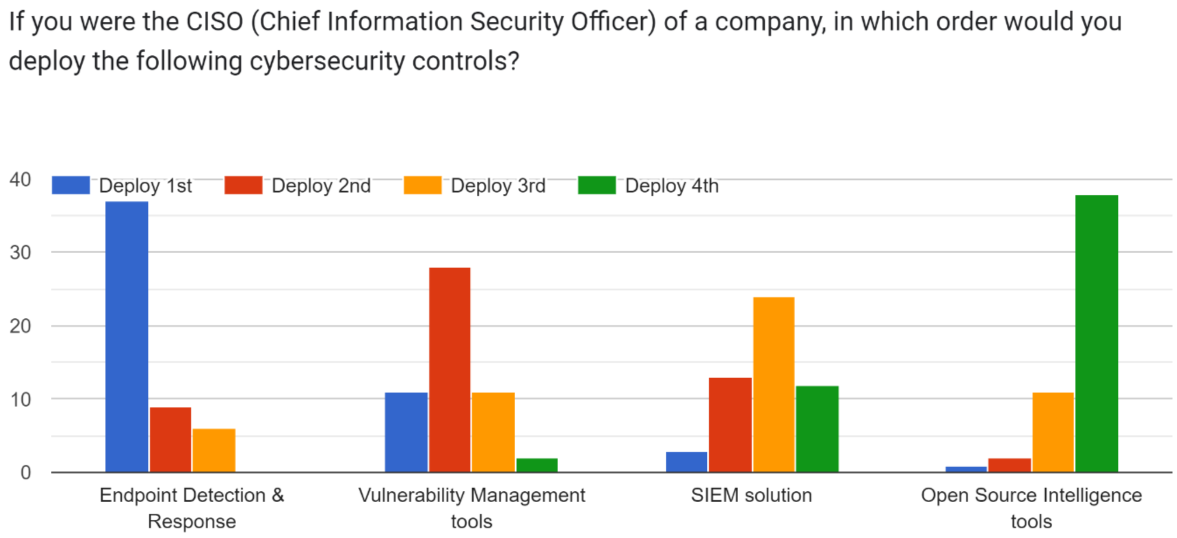
Question 13 queries the participant on whether they understand the efforts in terms of time and cost to maintain Open Source Intelligence tools? (OSINT)


Do you understand the efforts in terms of time and cost to maintain Open Source Intelligence tools?

52 responses

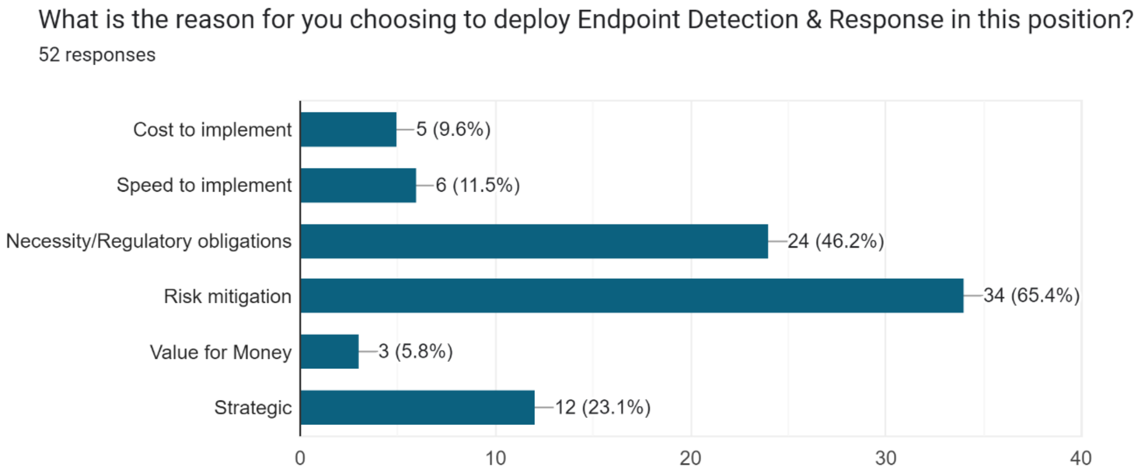
- The majority of participants in my survey did not understand the efforts to maintain this solution.

Question 14 put the participant in the role of CISO and asks in what order would they roll out the cybersecurity solutions.


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

- Mixed results across this question and a lot to consider. However, the main takeaways are that EDR got the most “Deploy 1st” votes, VM scanning tools got the most “Deploy 2nd votes”, SIEM got the most “Deploy 3rd votes” and OSINT got the most “Deploy 4th” votes. This was largely in line with my own recommendations after evaluation.

Question 15 asked for the reasons for putting EDR into this deployment position.

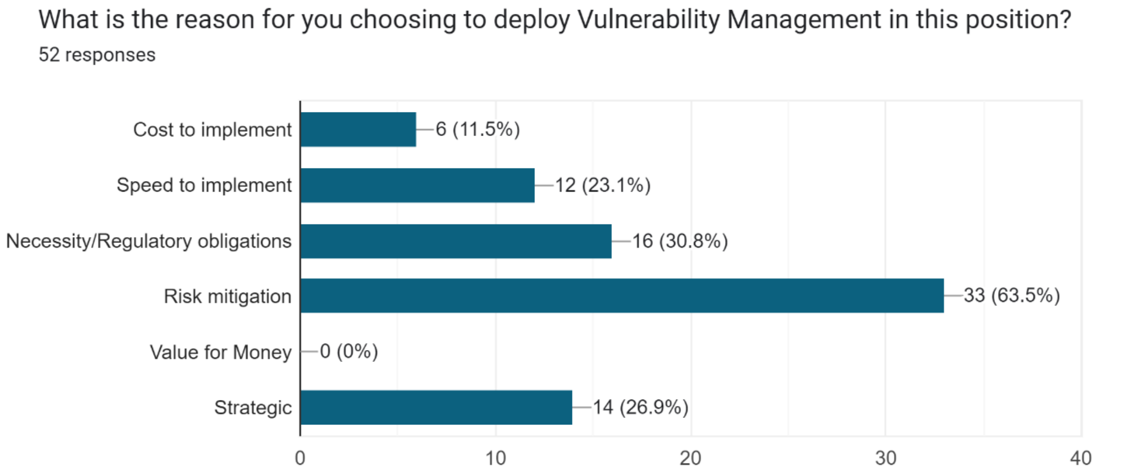


What is the reason for you choosing to deploy Endpoint Detection & Response in this position?

52 responses

- Risk mitigation was the clear first choice here, although this was the chosen reason for all of the first 3 cybersecurity solutions.

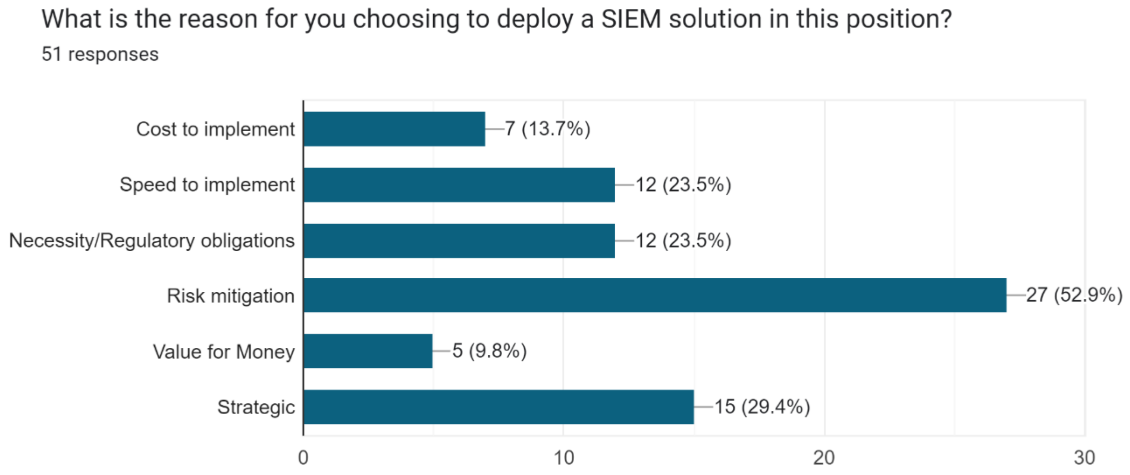
Question 16 asked for the reasons for putting VM scanning into this deployment position.



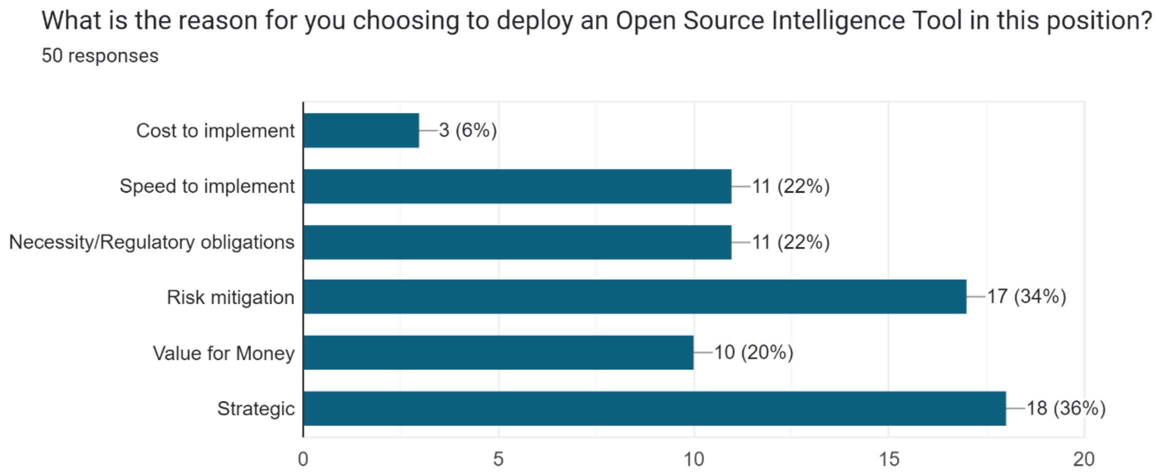
What is the reason for you choosing to deploy Vulnerability Management in this position?

52 responses

Question 17 asked for the reasons for putting SIEM solution into this deployment position.



Question 18 asked for the reasons for putting OSINT into this deployment position.



- Interestingly, the main reason chosen for this was strategic, although it is difficult to read too much into this.

6 References

Checkpoint, 2022. *EDR vs Antivirus - What's The Difference?.* [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 24 July 2022].

Fitzpatrick, J., 2018. *Everything you wanted to know about contracting but were too afraid to ask – part on.* [Online]
Available at: https://www.sureskills.com/Resources/Archive/ArtMID/1968/ArticleID/5/Everything-you-wanted-to-know-about-contracting-but-were-too-afraid-to-ask-%E2%80%93-part-one
[Accessed 02 July 2022].

RedLegg, 2019. *WHAT IS VULNERABILITY SCANNING, AND HOW DOES IT WORK?.* [Online]
Available at: https://www.redlegg.com/blog/what-is-vulnerability-scanning-and-how-does-it-work
[Accessed 09 April 2022].

Rosencrance, L., 2020. *security information and event management (SIEM).* [Online]
Available at: https://www.techtarget.com/searchsecurity/definition/security-information-and-event-management-SIEM
[Accessed 30 March 2022].

Software Testing Help, 2022. *Top 11 Most Powerful CyberSecurity Software Tools In 2022.* [Online]
Available at: https://www.softwaretestinghelp.com/cybersecurity-software-tools/
[Accessed 19 July 2022].

Tennessee State Government, 2022. *Inherent and Residual Risk.* [Online]
Available at: https://www.tn.gov/content/dam/tn/finance/accounts/Inherent-vs-RisidualRisk.pdf
[Accessed 13 June 2022].

Wikipedia, 2022. *Vulnerability scanner.* [Online]
Available at: https://en.wikipedia.org/wiki/Vulnerability_scanner
[Accessed 07 April 2022].

Wright, G., 2022. *What is endpoint detection and response (EDR)?.* [Online]
Available at: https://www.techtarget.com/searchsecurity/definition/endpoint-detection-and-response-EDR
[Accessed 22 June 2022].