National College of Ireland

Configuration Manual

MSc Research Project
Masters in Cybersecurity

Megan Haybyrne
Student ID: X21189439

School of Computing
National College of Ireland

Supervisor: Mark Monaghan

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Megan Haybyrne
Student ID:	X21189439
Programme:	Msc Research Project **Year:** Msc add on - 2023
Module:	Masters in Cybersecurity
Lecturer:	Mark Monaghan
Submission Due Date:	14th August 2023
Project Title:	An Investigation into the Benefits of Risk Management & Monitoring to aid Cybersecurity in an SME
Word Count:	1200 **Page Count: 11.**

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: Megan Haybyrne

Date: 12th August 2023

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.

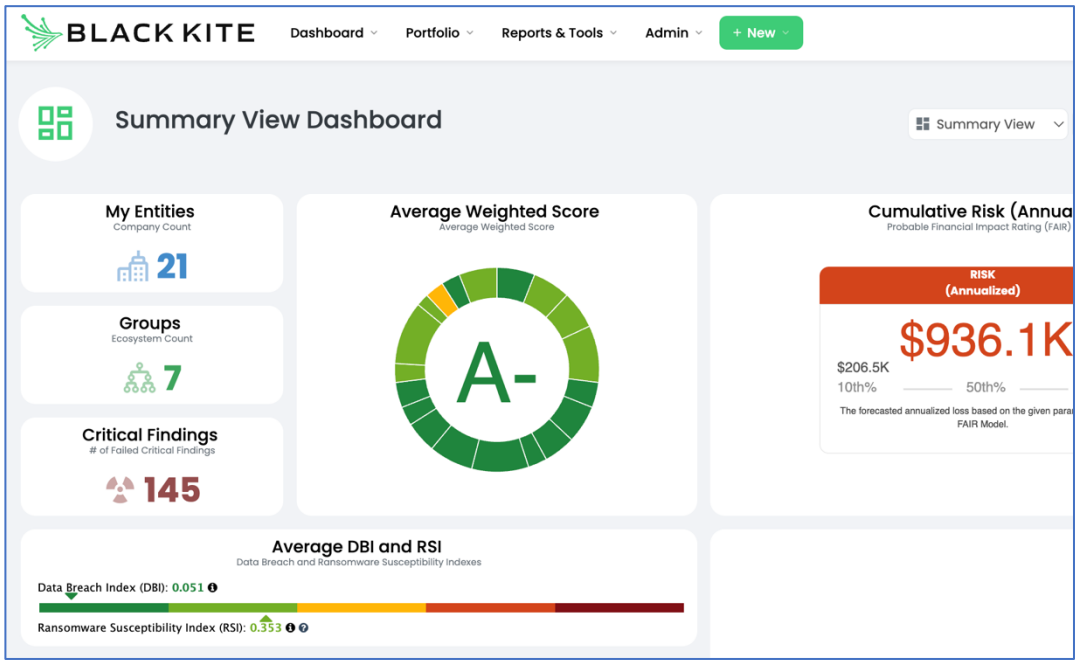
Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Megan Haybyrne
Student ID: X21189439

1 Black Kite Configuration

As discussed in the research report, Black Kite is a tool used to scan the externally facing assets of a company. This is an Open-source Threat Intel Tool (OSINT) and can be used to scan a company by anyone that knows their web domain.

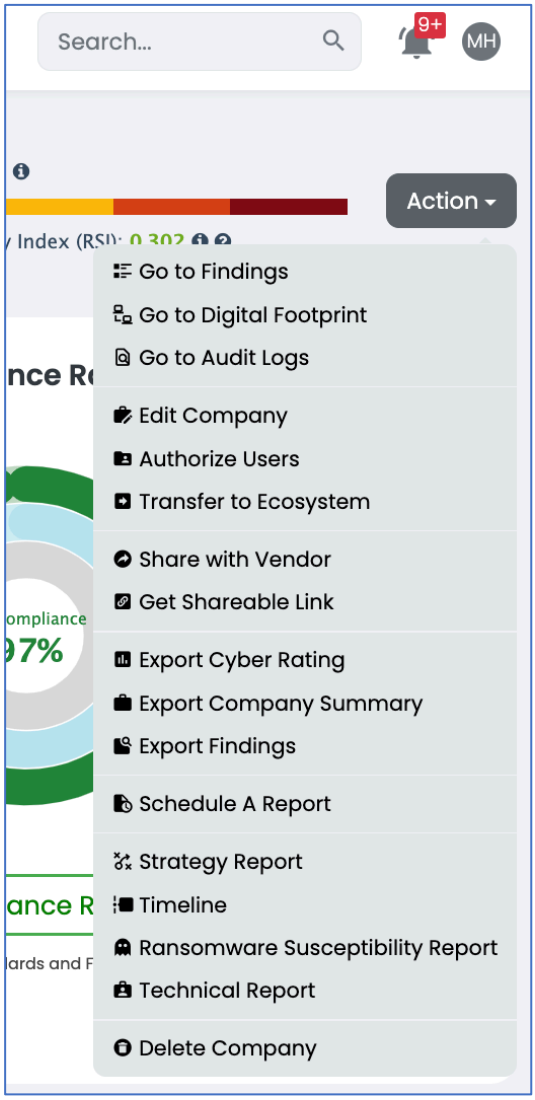


The below steps were used to setup and pull information on the companies used in this project:

- Log into Black kite.
- Click **Add** in the top of the screen, add the company domain (e.g., NCI.ie) and give it at least twenty-four hours to pull together the data.
- In the search section, enter the company name to navigate to their Black Kite page.
- This brings you to the dashboard where you can see an overview of the OSINT report for this company. The information in the KPI showing the External view and External changes is derived from here.

- There is also a section to pull multiple reports, screenshots were taken from these sections also. This is not included as it isn't possible to hide the company name.

- For example, on the right-hand side of the dashboard select Actions, from the drop-down menu select strategy report. This is where the external improvement strategy information is derived from in the screen-snip.



2 Cynomi

Cynomi is used to run through relevant questions with the clients in question and generates the results of the GAP Analysis. This is then used to log risks in the chosen risk management system.

The below steps are used for this process:

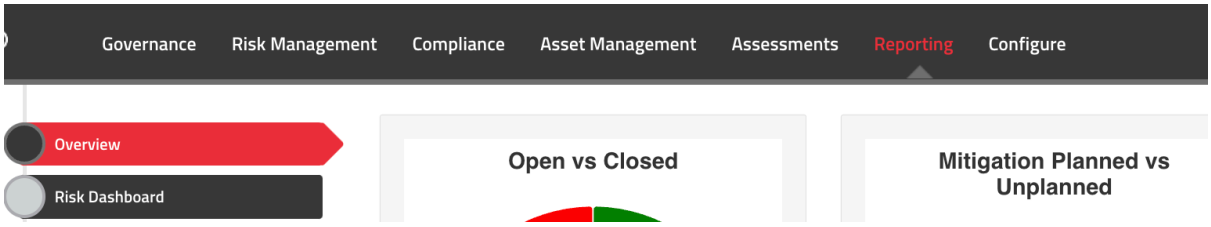
- Log into the Cynomi platform.
- Select company you want to evaluate or generate reports on.
- Once in the chosen company's portal, navigate to the assessment section & run through any sections that are relevant to the company (e.g., asset management, email security, etc). with every assessment complete, tasks will populate and be listed as complete, partially complete and not done and a score will begin to be generated.
- Once ready, navigate to the right corner of the dashboard click on download to generate the required report.
- Screenshots can be pulled from the dashboard or from the available reports.
- The dashboard provides the ability to filter based on risk type (Data Leak, Website Defacement, Ransomware, Fraud). This is useful in reporting also and can be used in the KPI report. See an example output below.

3 Risk Management System Exports

3.1 SimpleRisk

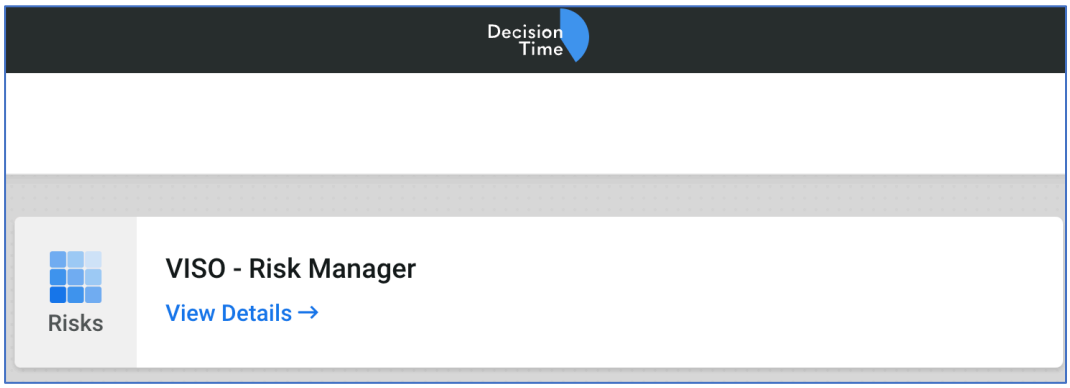
SimpleRisk is used to log risks for Healthcare Company 1.
It provides a platform to log and monitor the quantity of inherent and residual risks and has a range of reporting and filtering options that allow for detailed exports and risk analyses.

- To export the data required for the KPI Report, first navigate to the SimpleRisk platform.
- Select **Reporting** at the top of the window.
- Select Dynamic Risk Report from left column – this gives the option to export the risk list, filtered by company and residual risk, which is counted and used in the KPI summary page.
- Click on the ID to get more information about the risk if required.
- The Overview & Risk Dashboard columns can also be selected to provide the graphs and pie charts that are included in the Healthcare Company 1 Excel.



3.2 DecisionTime

Log into DecisionTime and navigate to the Risk Section.



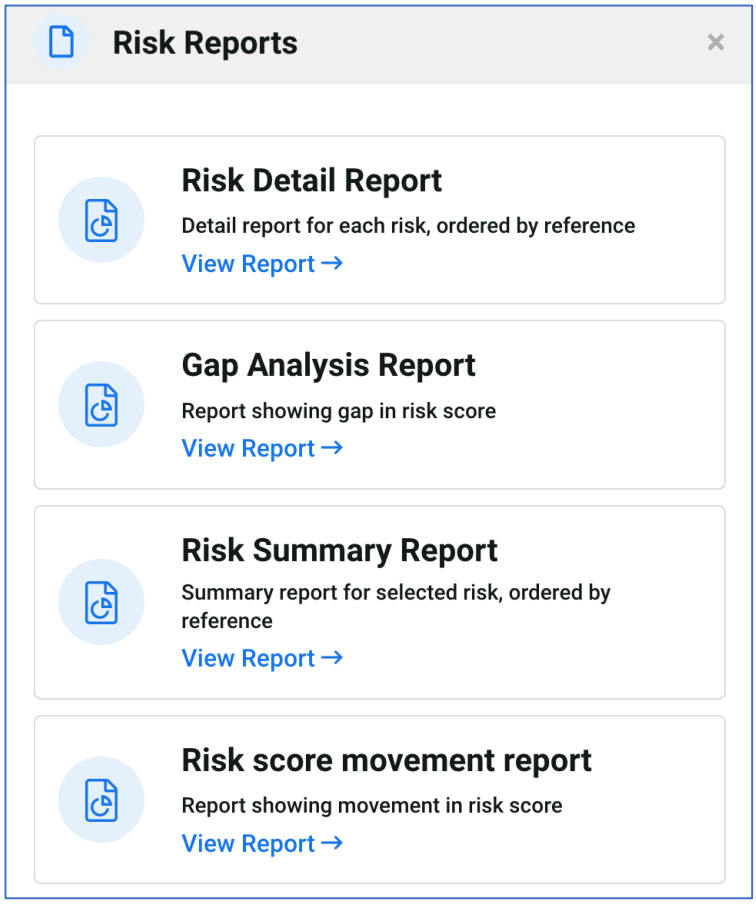
From here, you can filter by client & export a range of risk reports.

The statistics that are included in the Excels for IT company 1 is derived from the dashboard after the relevant filters were applied.

Filters:

- Entity: IT Company 1
- All Risks

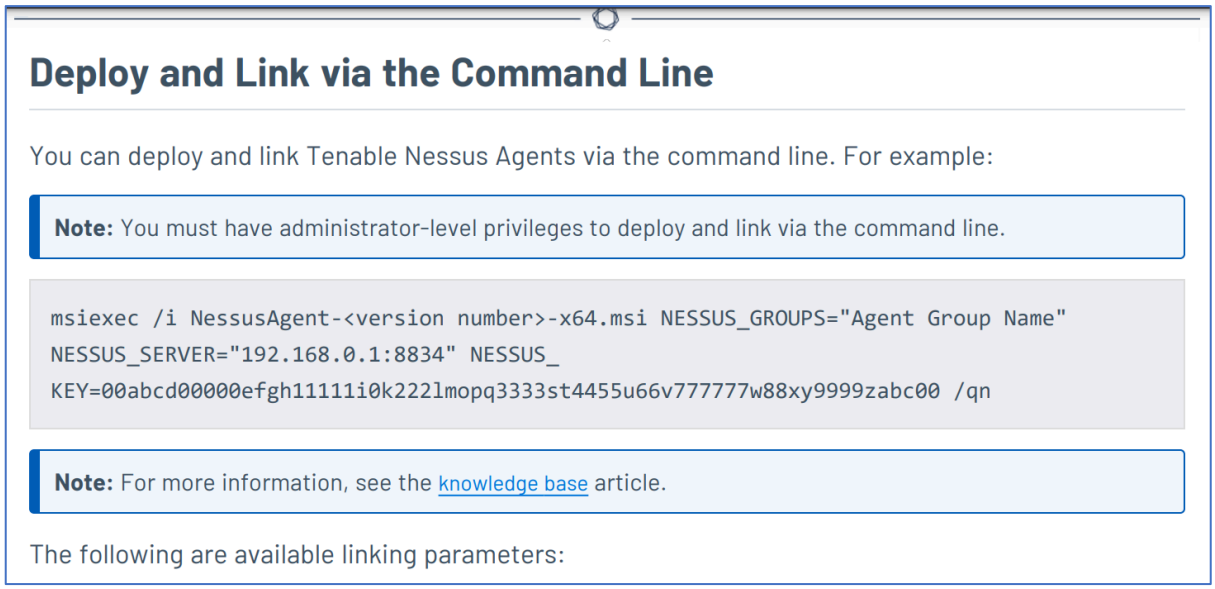
Additional information can also be gathered through the different exportable report options. For the sake of this project, I decided not to include such reports as they make it difficult to anonymise the companies I'm discussing. In a normal situation, I would incorporate further details from the reports.



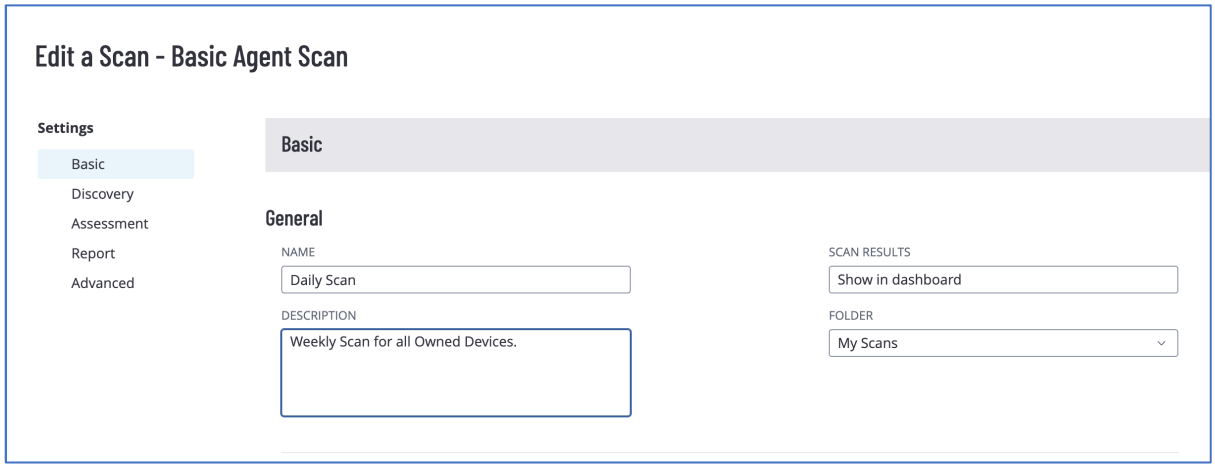
4 Vulnerability Management

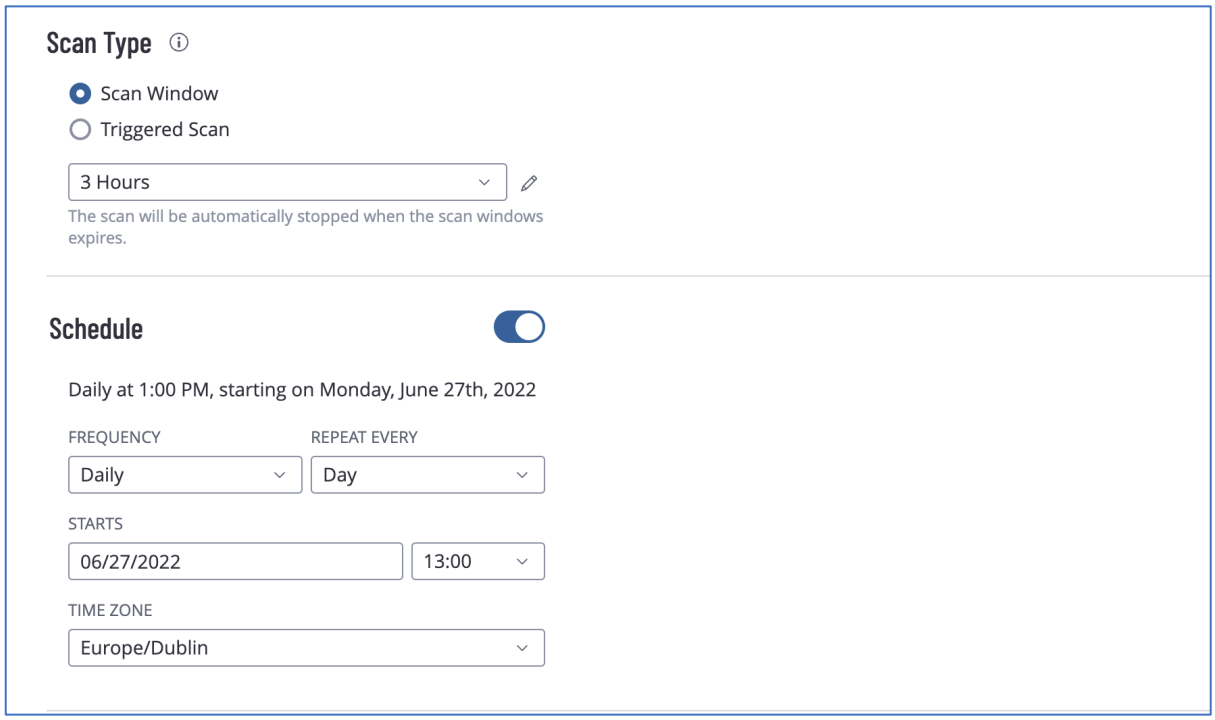
The internal scanning tool used for this project is a vulnerability management tool called Tenable IO. To setup this up, this requires setting up a Tenable Agent on each device you want to monitor and then linking this agent to the Tenable IO instance that will be scanning and reporting such devices.

Once the above has been configured, using the below configurations, the scanning and reporting functionality can be used.



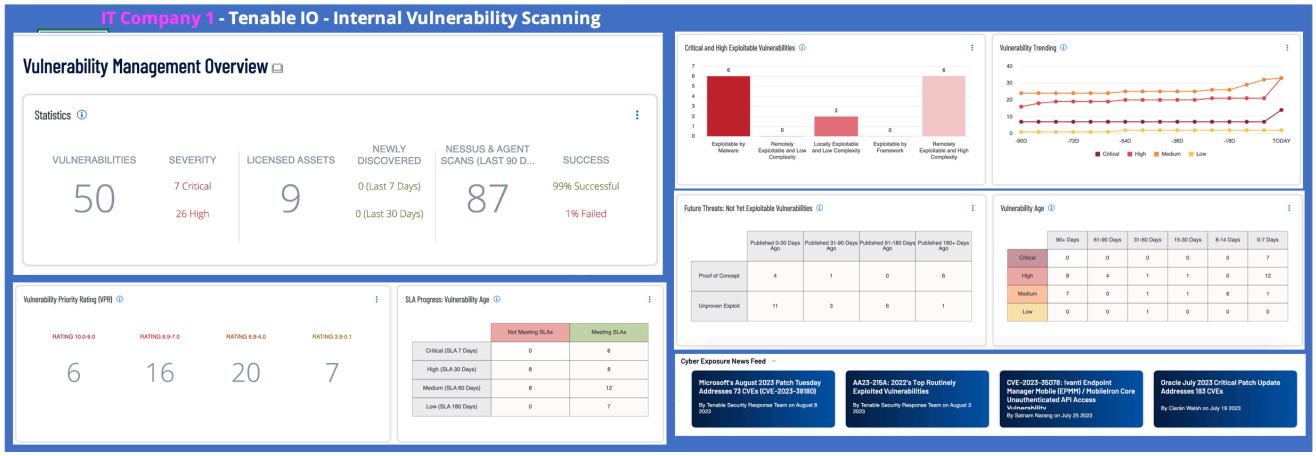
Once the agents are successfully installed, a scan is scheduled to run daily on the system.

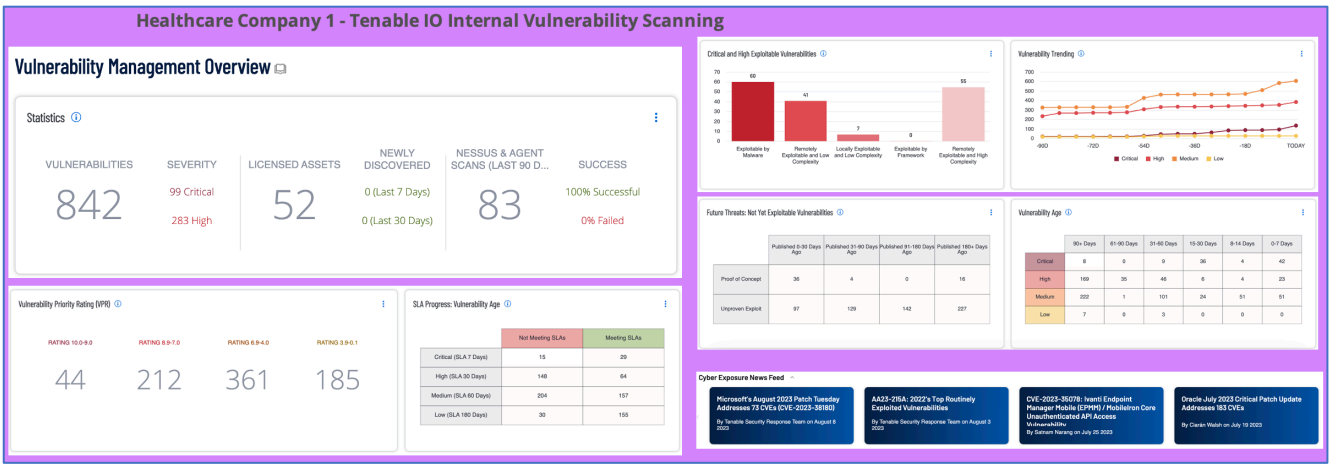




Once the above settings were in place, and at least one full scan had run, I began gathering the information for my reports. The below steps summarise how I did this.

- Navigate to the company in Tenable by going to the top left menu, select account, click on company name, right click, and select sign in.
- Click into the vulnerability section.
- This section is where I pulled the relevant screenshots for the company excels, that feed into the statistics I summary in the KPI report that I generated for this project.





5 References

- *Tenable, inc.*. Available at: https://docs.tenable.com/vulnerability-management/Content/PDF/Tenable_Vulnerability_Management-User_Guide.pdf (Accessed: 01 August 2023).
- *Welcome to tenable nessus agent 10.4.X* (no date) *Welcome to Tenable Nessus Agent 10.4.x (Tenable Nessus Agent 10.4)*. Available at: https://docs.tenable.com/nessus-agent/10_4/Content/GettingStarted.htm (Accessed: 01 August 2023).