

# 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:** 14<sup>th</sup> 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:** 12<sup>th</sup> August 2023

**PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST**

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

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

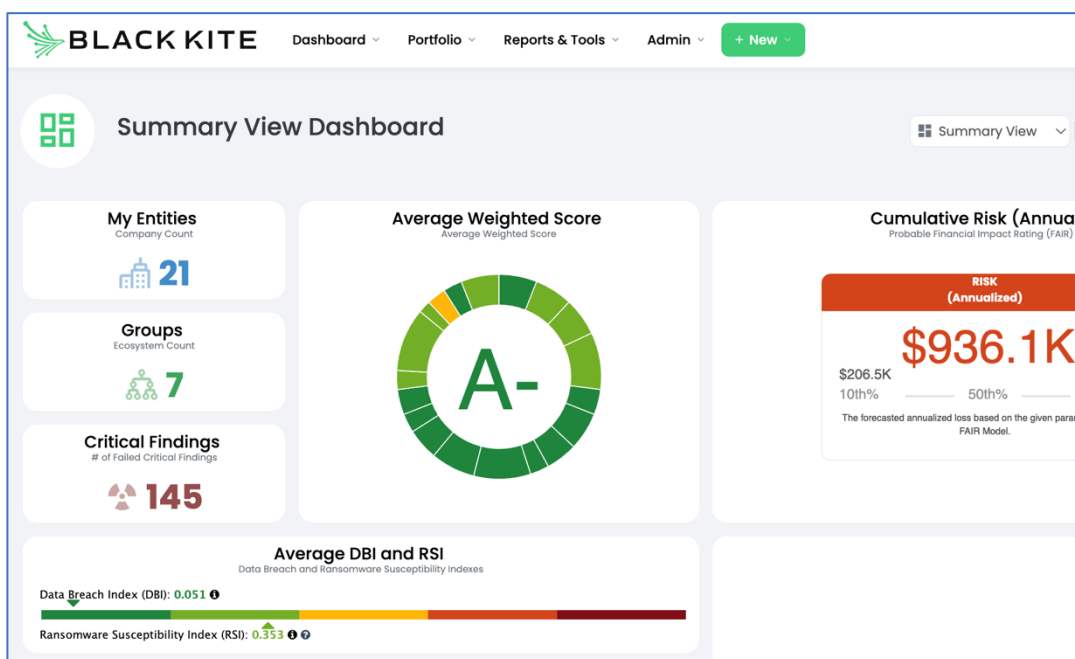
<b>Office Use Only</b>	
Signature:	
Date:	
Penalty Applied (if applicable):	

# Configuration Manual

Megan Haybyrne  
Student ID: X21189439

## 1 Black Kite Configuration

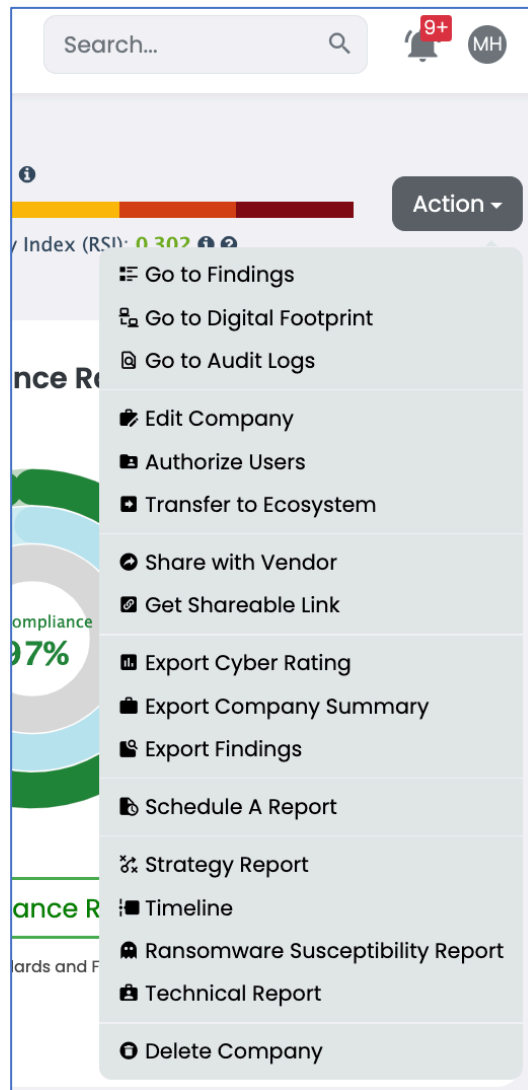
As discussed in the research report, Black Kite is a tool used to scan the externally facing assets of a company. This is an Open-source Threat Intel Tool (OSINT) and can be used to scan a company by anyone that knows their web domain.



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.

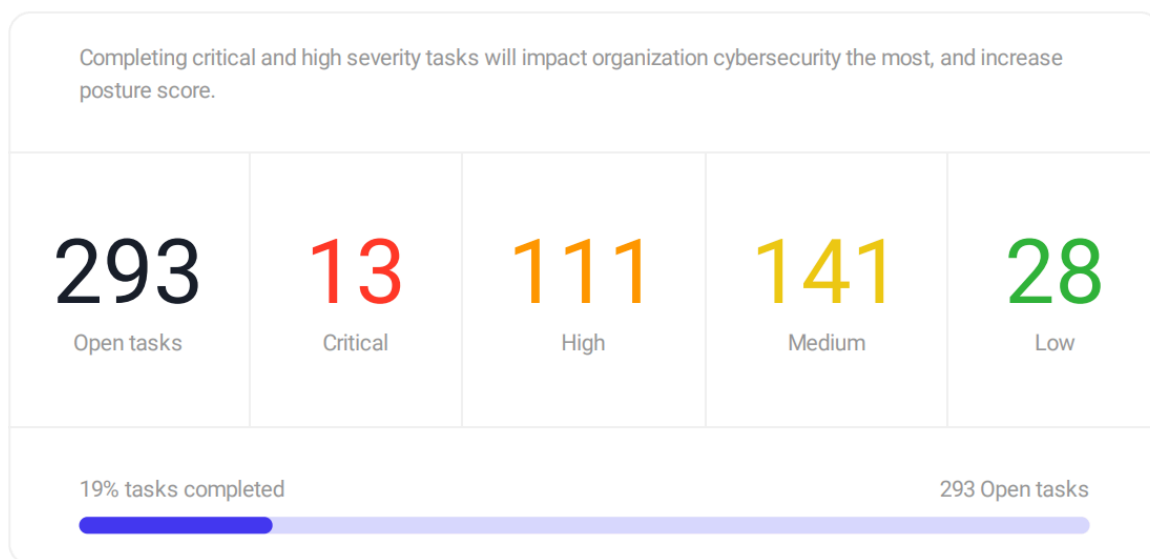


## 2 Cynomi

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.



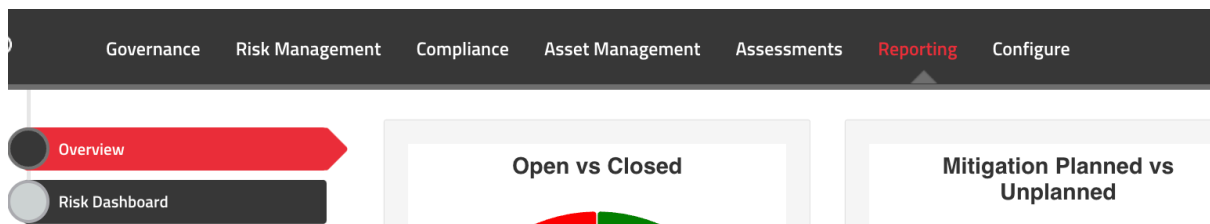
### 3 Risk Management System Exports

#### 3.1 SimpleRisk

SimpleRisk is used to log risks for Healthcare Company 1.

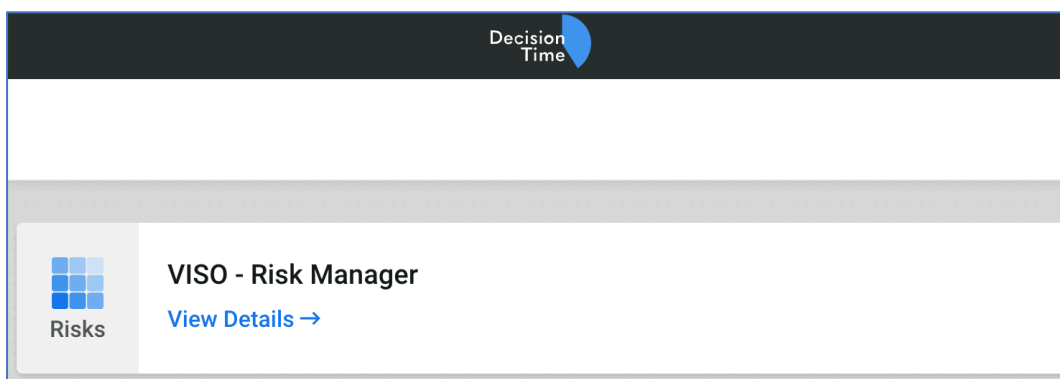
It provides a platform to log and monitor the quantity of inherent and residual risks and has a range of reporting and filtering options that allow for detailed exports and risk analyses.

- 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.

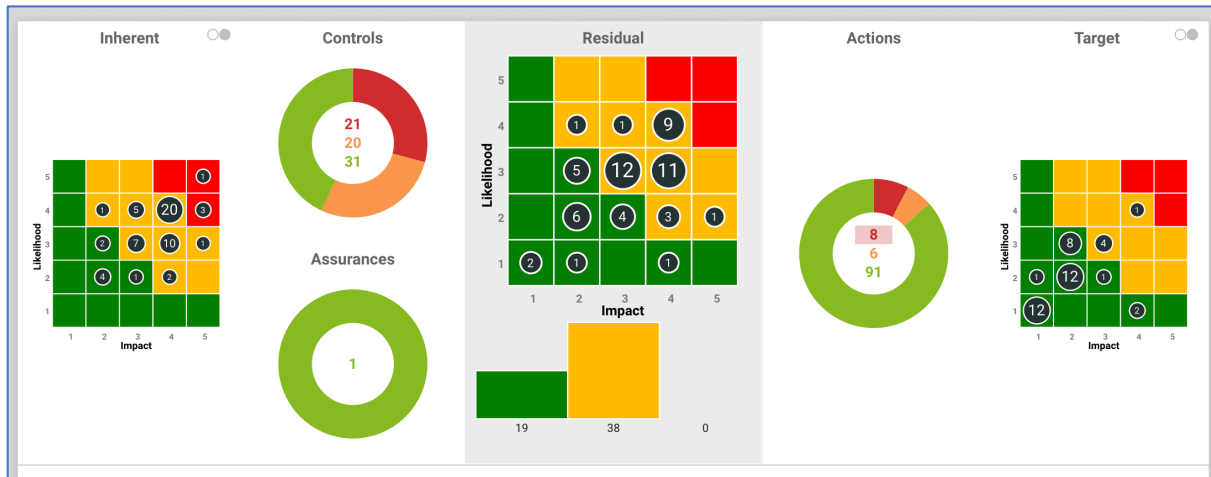


From here, you can filter by client & export a range of risk reports.

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.

📄 Risk Reports
✕

📄

**Risk Detail Report**

Detail report for each risk, ordered by reference

[View Report →](#)

📄

**Gap Analysis Report**

Report showing gap in risk score

[View Report →](#)

📄

**Risk Summary Report**

Summary report for selected risk, ordered by reference

[View Report →](#)

📄

**Risk score movement report**

Report showing movement in risk score

[View Report →](#)

## 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.

### Deploy and Link via the Command Line

You can deploy and link Tenable Nessus Agents via the command line. For example:

**Note:** You must have administrator-level privileges to deploy and link via the command line.

```
msiexec /i NessusAgent-<version number>-x64.msi NESSUS_GROUPS="Agent Group Name"  
NESSUS_SERVER="192.168.0.1:8834" NESSUS_  
KEY=00abcd0000efgh11111i0k222lmopq3333st4455u66v77777w88xy9999zabc00 /qn
```

**Note:** For more information, see the [knowledge base](#) article.

The following are available linking parameters:

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

### Edit a Scan - Basic Agent Scan

**Settings**

- Basic
- Discovery
- Assessment
- Report
- Advanced

**Basic**

**General**

NAME:

DESCRIPTION:

SCAN RESULTS:

FOLDER:



### Scan Type ?

Scan Window  
 Triggered Scan

3 Hours ✎

The scan will be automatically stopped when the scan windows expires.

---

### Schedule ☑

Daily at 1:00 PM, starting on Monday, June 27th, 2022

FREQUENCY:  REPEAT EVERY:

STARTS:

TIME ZONE:

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.

**IT Company 1 - Tenable IO - Internal Vulnerability Scanning**

#### Vulnerability Management Overview

Statistics

VULNERABILITIES	SEVERITY	LICENSED ASSETS	NEWLY DISCOVERED	NESSUS & AGENT SCANS (LAST 90 D...)	SUCCESS
50	7 Critical 26 High	9	0 (Last 7 Days) 0 (Last 30 Days)	87	99% Successful 1% Failed

Vulnerability Priority Rating (VPR)

RATING 10.0-9.0	RATING 8.9-7.0	RATING 6.9-4.0	RATING 3.9-0.1
6	16	20	7

SLA Progress: Vulnerability Age

	Not Meeting SLAs	Meeting SLAs
Critical (SLA 7 Days)	0	6
High (SLA 30 Days)	8	8
Medium (SLA 60 Days)	8	12
Low (SLA 180 Days)	0	7

Critical and High Exploitable Vulnerabilities

Exploitable by Nessus	Remotely Exploitable and Low Complexity	Locally Exploitable and Low Complexity	Exploitable by Framework	Remotely Exploitable and High Complexity
6	0	2	0	8

Vulnerability Trending

Future Threats: Not Yet Exploitable Vulnerabilities

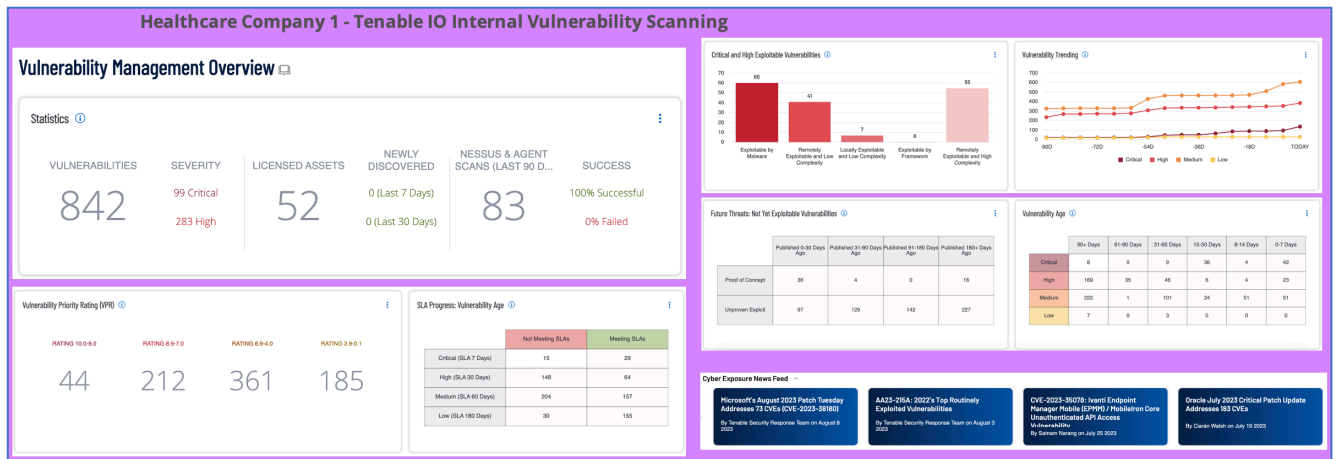
	Published 0-30 Days Ago	Published 31-60 Days Ago	Published 61-180 Days Ago	Published 180+ Days Ago
Proof of Concept	4	1	0	6
Unpatched Exploit	11	3	6	1

Vulnerability Age

	90+ Days	61-90 Days	31-60 Days	10-30 Days	8-14 Days	0-7 Days
Critical	0	0	0	0	0	7
High	0	4	1	1	0	12
Medium	7	0	1	1	0	1
Low	0	0	1	0	0	0

Cyber Exposure News Feed

- Microsoft's August 2022 Patch Tuesday Addresses 73 CVEs (CVE-2022-36860) by Tenable Security Response Team on August 9, 2022
- AA25-216A: 2022's Top Routinely Exploited Vulnerabilities by Tenable Security Response Team on August 3, 2022
- CVE-2022-36278: Invali Endpoint Manager Hosts (EMH) /Redirection Core Unauthenticated API Access Vulnerability by Soroush Nazari on July 25, 2022
- Oracle: July 2022 Critical Patch Update Addresses 183 CVEs by Cisco Walsh on July 19, 2022



## 5 References

- *Tenable, inc..* Available at: [https://docs.tenable.com/vulnerability-management/Content/PDF/Tenable\\_Vulnerability\\_Management-User\\_Guide.pdf](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](https://docs.tenable.com/nessus-agent/10_4/Content/GettingStarted.htm) (Accessed: 01 August 2023).