MIS 781-BUSINESS INTELLIGENCE AND DATABASE

Business Intelligence Solution Development and Report

Prepared by:

Sachin Bhat (218676233)

Table of Contents

1. Introduction

A Cyber Security department in an organisation has a very important role to play. They make sure that the company's data is protected from cyber-attacks, leaks, and other form of threats. Usually their work involves performing risk assessment, developing and implementing security strategies and planning, establishing security policies and procedures, developing incident response and management plans, ensuring network and infrastructure security, implementing data protection measures, conducting security awareness and training campaigns, deploying threat intelligence and security monitoring tools, performing vulnerability management, reporting security incidents, building a sturdy security architecture and more.

Visualisations hold utmost significance when presenting reports. They enable quick data interpretation to identify patterns and derive insights. Data can be explored by interacting with these visualisations thereby providing a deeper understanding. They make it possible to elaborate huge amounts of data to the audience through easy storytelling. Visualisations enable collaboration with other people in the organization, sharing of data, real-time data monitoring and strongly backed decision making.

This report has been formed while being focused on these grounds. It aims to present valuable information to a cyber security department and high-ranking individuals of a company through visualisations which have been generated using Power BI. Three different databases were created and worked upon to generate dashboards. These databases were named:

1. Cyber Security Sales Data
2. Cyber Security Incidents Data
3. Network Traffic Data

1.1 Objectives of the BI Dashboards

Cyber Security Sales Data:

This dashboard has been created to assist the head CSO (Chief Sales Officer) and cyber security sales departments of several companies under one parent company. It keeps a track of the product sales by product type across different regions around the globe. This dashboard makes it easier to track the type of product a particular company is selling and the revenue it has generated. It assists the organisation to monitor and work on areas they are lacking behind.

Cyber Security Incidents Data:

This dashboard has been specifically designed to assist the CISO (Chief Information Security Officer) and the cyber security team of a company having its operations in different countries. The main objective of this dashboard is to highlight the impact of security incidents and the loss it had caused to the organisation. This dashboard keeps a track of the cyber-attacks that have been made on the company across the world along with the Incident ID, date, and timestamp.

Network Traffic Data:

This dashboard has been specifically created to aid the Network Administrator of the organisation. It keeps a track of the data exchange (interaction) between computer systems using different protocols within the organisation as well as with computer systems outside the organisation to determine whether an attack took place or not. Date and timestamps provide exact details of the data transfer and cyber attack's confirmation.

1.2 Benefits of the BI Dashboards

Cyber Security Sales Data:

This dashboard is extremely useful to the head CSO of the organization. It provides insights on how different companies are performing based on several filters. It would be very handy when the goal is to identify the total sales based on the company name, product name, product type, region, industry, and sales representative. Also, this will highlight the companies or products that are not generating enough sales and require more attention. Based on those insights, the management would come up with the suitable strategies to tackle the situation and increase sales to keep up and stay ahead of the competition. This dashboard also highlights sales representatives' performances and can be utilised to provide them with bonuses and motivation to do even better.

Cyber Security Incidents Data:

This dashboard comes in super handy for the CISO and the cyber security department of the company to keep a track of the reported cyber incidents on the organisation. This dashboard assists in focusing on the countries along with its cities which faced cyber-attacks. It brings forth each industry which faced the attack along with type of threat and the attack vector used to carry out the attack. It also highlights the target data and the severity of impact along with the monetary loss it caused to the organisation. This will enable the higher-ups to realise which areas require immediate attention and work on strengthening the security architecture against the threat types and attack vectors that are dangerous. Learnings using this will allow the company to prevent such attacks in the future.

Network Traffic Data:

The Network Administrator and their team can make efficient use of this dashboard. It makes it easier to track the computer system that faced or caused the attack by tracking its IP address and source port thereby enabling the engineers to establish whether an attack has occurred or not. It specifies the protocol used for data exchange and if that exchange involved a cyber-attack. Using this, the network management will be able to establish which protocol is safer to use and which one is not thereby safeguarding company's network.

1.3 Assumptions

Cyber Security Sales Data:

- All companies operate under one parent company.
- This represents weekly sales data for 10 sub companies during the month of January for the year 2022 and is being utilised by the CSO (Chief Sales Officer) to increase sales.
- Product name is a sub-category of product type.
- Sales are in USD.

Cyber Security Incidents Data:

- This represents complete details about cyber security incident that have taken place in the year 2022 and is being utilised by the CISO (Chief Information Security Officer) to strengthen company's cyber security architecture.
- Attacks have occurred in a repeated manner i.e., on the 1st of every month between January and October.
- Attack Vector is a sub-category of threat type.
- Attack Vector is the medium used to carry out the attack.

Network Traffic Data:

- This data represents the year 2022 and lies between January and October.
- Time represents timestamp of suspicious data exchange.
- This represents company's data about bytes sent/received and whether it involved an attack or not.
- All 3 protocols are used in data exchange.
- Data exchange (interaction) through computer systems is happening among as well as outside the organisation.

1.4 Description of business rules and of variables used in this report

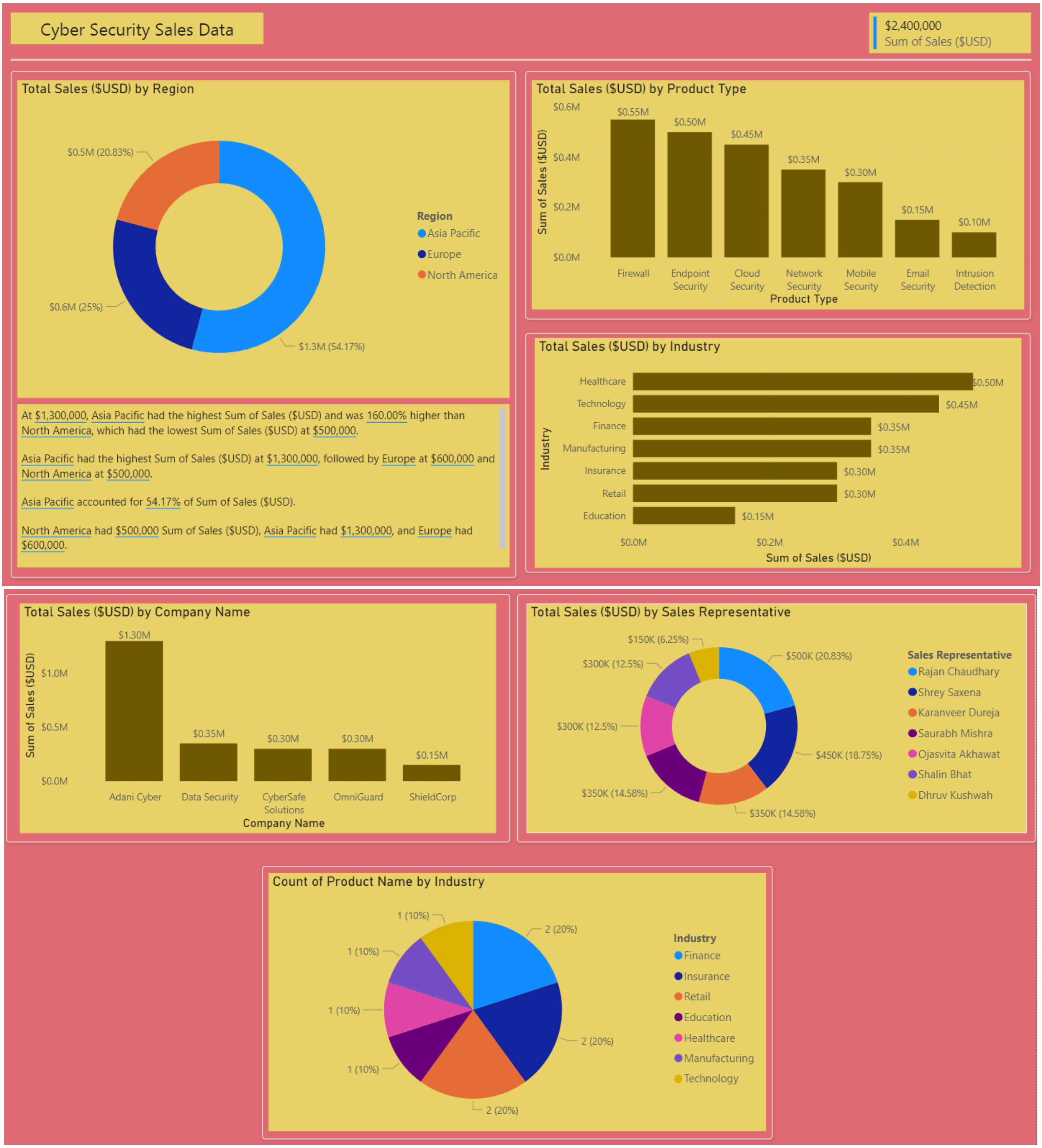
- All employees should arrive at their work locations at 9:00 A.M and must work at least 40 hours per week.
- Sales for the week are a result of daily reporting done through other Power BI dashboards.
- Incident ID will be automatically assigned to a cyber-attack as soon as it has been detected.
- The Impact has been predefined as per the Loss amount.
- There are 3 protocols involved in Network Traffic Data: TCP (Transmission Control Protocol), UDP (User Datagram Protocol), ICMP (Internet Control Message Protocol).

Variables	Data Type	Description
Company_Name	String	Company name
Product_Name	String	Product name
Product_Type	String	Product type
Sales_Representative	String	Salesperson
Incident_ID	Integer	Incident ID
Date	DATE	Date of incident and network traffic data exchange
Time	TIME	Time of incident and network traffic data exchange
Threat_Type	String	Type of threat
Attack_Vector	String	Medium of attack
Source_IP	String	Source IP of affected system
Protocol	String	Protocol used for tata transfer
Source_Port	Integer	It identifies how the data is being transferred
Bytes Sent	Integer	Bytes sent while network interaction
Bytes Received	Integer	Bytes received while network interaction

Attack_Detected	String	Whether the attack was detected or not

2. BI Dashboards

2.1 Cyber Security Sales Data Dashboard for the CSO



At $1,300,000, Asia Pacific had the highest Sum of Sales ($USD) and was 160.00% higher than North America, which had the lowest Sum of Sales ($USD) at $500,000.

Asia Pacific had the highest Sum of Sales ($USD) at $1,300,000, followed by Europe at $600,000 and North America at $500,000.

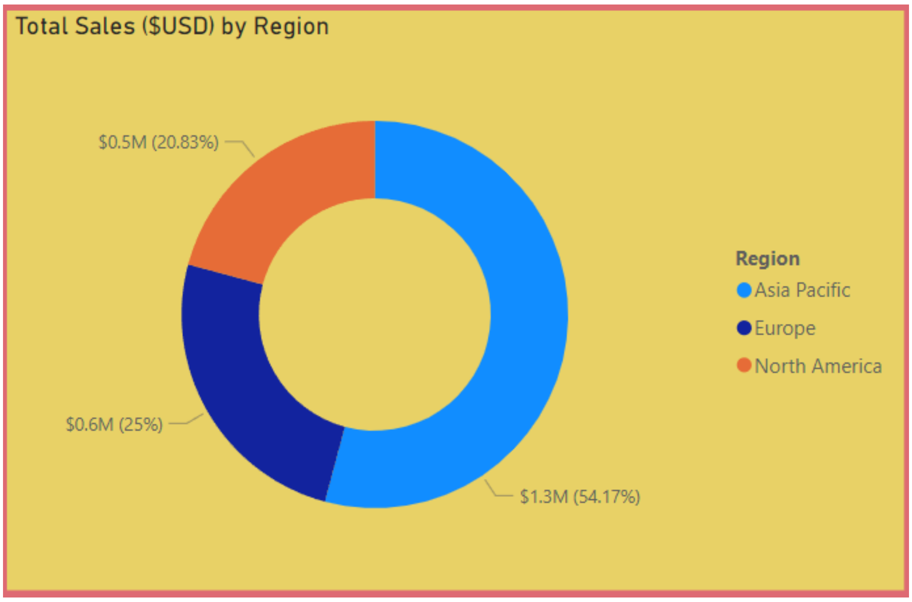
Asia Pacific accounted for 54.17% of Sum of Sales ($USD).

North America had $500,000 Sum of Sales ($USD), Asia Pacific had $1,300,000, and Europe had $600,000.

This dashboard represents the weekly sales data of cyber security products for a company. The overall sales of all products across all regions amounts to $2,400,000.

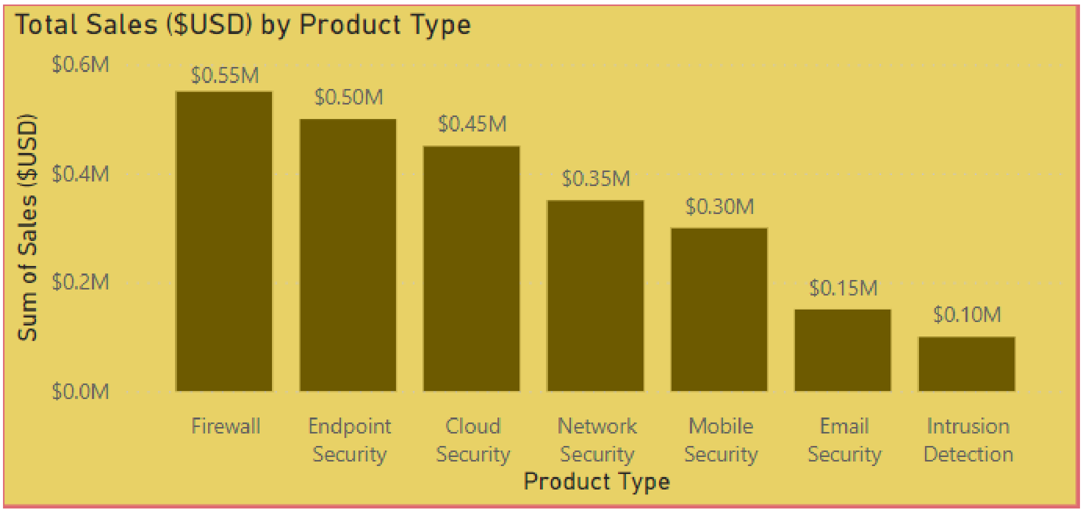
Asia Pacific had the total sales of $1.3 million which was generated using three product types and from three separate industries. Endpoint Security products from the Healthcare industry contributed by $0.50 million. Cloud Security products from the Technology industry contributed by $0.45 million. Network Security products from the Manufacturing industry contributed by $0.35 million. **Europe** had the total sales of $0.6 million which was generated using three product types and from two separate industries. Firewall products from the Retail industry contributed by $0.20 million whereas Intrusion Detection products from the retail industry contributed by $0.10 million. Mobile Security products from the Insurance industry contributed by $0.30 million. **North America** had the total sales of $0.5 million which was generated using 2 product types and from two different industries. Firewall products from the Finance industry contributed by $0.35 million whereas Email Security products from the Education industry contributed by $0.15 million.

Chart 1



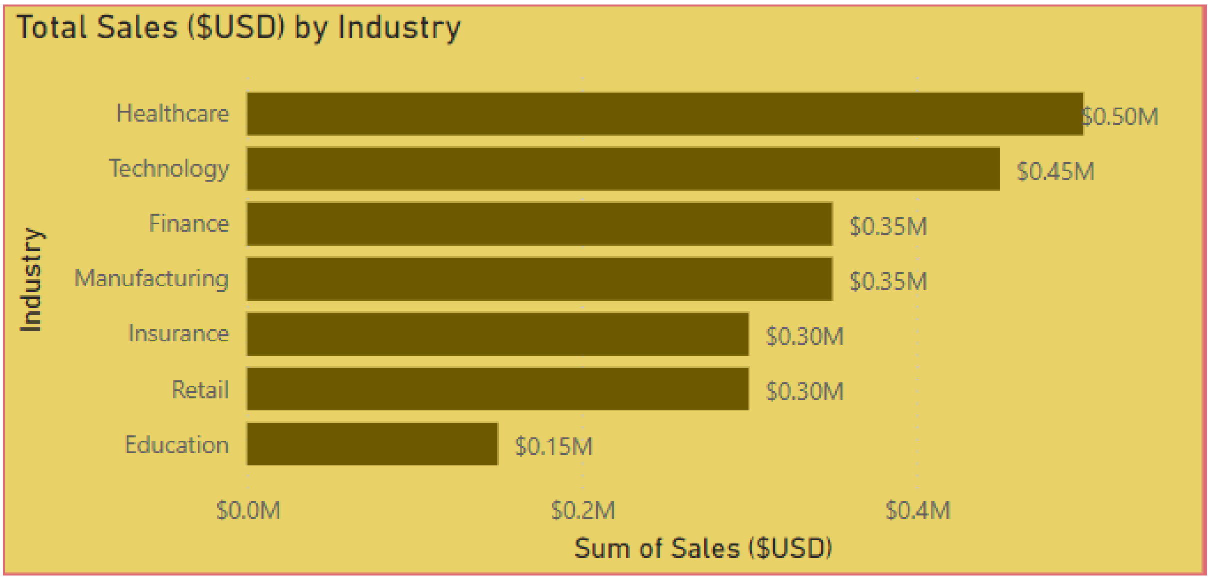
This donut chart appropriately represents total region wise sales of the head organisation. There are 3 regions across which the company sells its products. They are Asia Pacific, Europe, and North America. It can be observed that Asia Pacific region had the highest total sales which was $1.3 million. Europe was at the second position with total sales of $0.6 million and was followed by North America which had the least sales of $0.5 million. Asia pacific contributed to 54.17% of the total sales. Meanwhile, Europe contributed to 25% and North America contributed to 20.83% of the total sales. Asia Pacific's total sales was 160% more than North America's total sales.

Chart 2



This stacked column chart clearly represents total sales of the head company on the basis of 7 Product Types. Firewall products generated a total revenue of $0.55 million. Endpoint Security products amounted to total revenue of $0.50 million. Cloud Security products brought in $0.45 million. Network Security products generated total sales of $0.35 million followed by Mobile Security products which amounted to total sales of $0.30 million. Email Security products generated a revenue of $0.15 million followed by Intrusion Detection product sales which amounted to $0.10 million. Firewall and Endpoint Security products brought in the highest income and profit when compared to Email Security and Intrusion Detection products which contributed less.

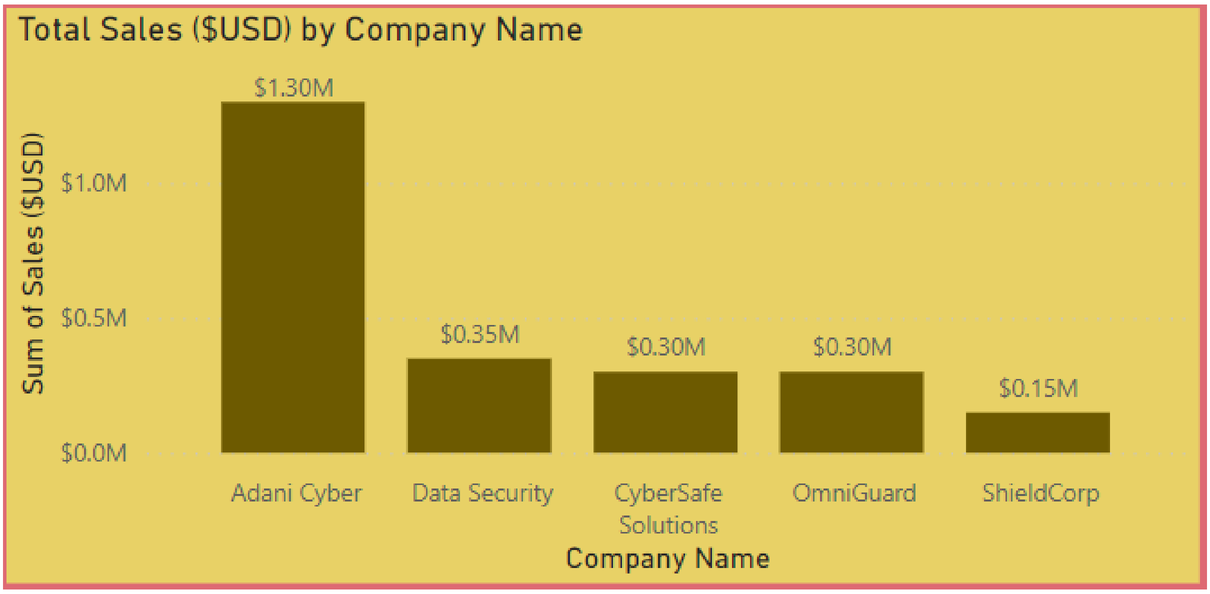
Chart 3



This clustered bar chart represents total sales of the head company on the basis of industry. Healthcare industry generated the highest number of sales with $0.50 million followed by the

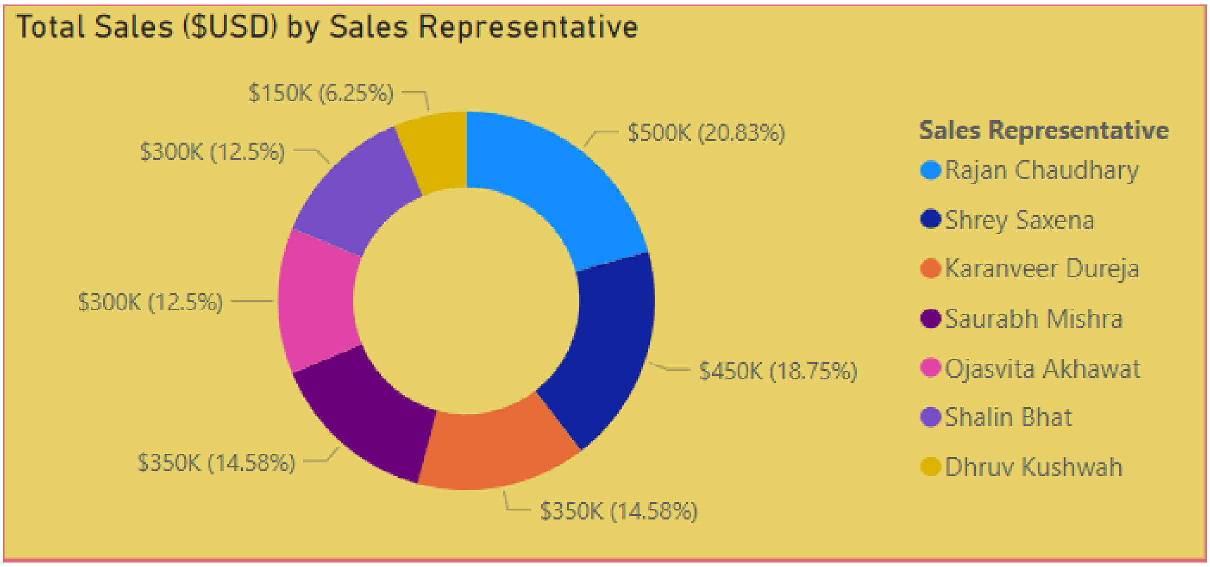
Technology industry which generated total sales of $0.45 million. Finance and Manufacturing industries come in line with sales number of $0.35 million each. They are followed by the Insurance and Retail industries which generated total revenues of $0.30 million each. Education industry brought in total sales of $0.15 million. Healthcare and Technology industries contributed hugely to the product sales meanwhile the Education industry contributed less.

Chart 4



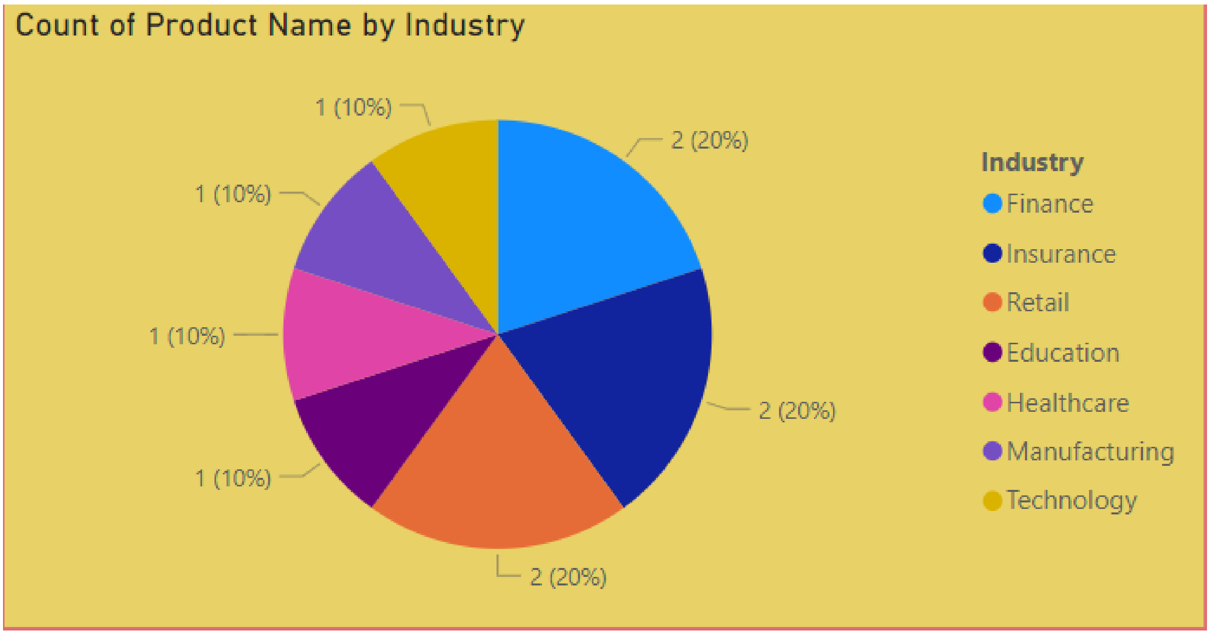
The stacked column chart perfectly represents total sales of the head organisation filtered by its sub-companies (company name). Adani Cyber generated sales of $1.30 million followed by Data Security which generated total sales of $0.35 million. The companies CyberSafe Solutions and OmniGuard generated total sales of $0.30 million each. ShieldCorp trails behind with a generated income of $0.15 million.

Chart 5



This donut chart appropriately depicts the income generated by different sales representatives. Sales representative Rajan Chaudhary contributed to 20.83% of total sales and brought in $500,000 followed by Shrey Saxena who contributed to 18.75% and brought in $450,000. Karanveer Dureja and Saurabh Mishra, each contributed to 14.58% of total sales and each of them generated a revenue of $350,000. Ojasvita Akhawat and Shalin Bhat, each contributed to 12.5% of total sales and each brought in a revenue of $300,000. Dhruv Kushwah contributed to 6.25% of total sales and generated an income of $150,000. Rajan and Shrey were the best performers.

Chart 6



This pie chart summarizes the products being used by different industries. Finance industry uses 20% of the products that belong to the Firewall domain. Insurance industry uses 20% of the products that belong to the Mobile Security domain. Retail industry makes use of 20% of the products where one belongs to Intrusion Detection and the other product belongs to the Firewall domain. Education industry uses 10% of the products which belongs to the Email security domain. Healthcare sector also uses 10% of the products and they belong to the Endpoint Security domain. Manufacturing sector uses 10% of the products which belongs to the Network Security domain. Technology sector makes use of Cloud Security domain and contributes by 10% as well.

2.2 Cyber Security Incidents Data Dashboard for the CISO

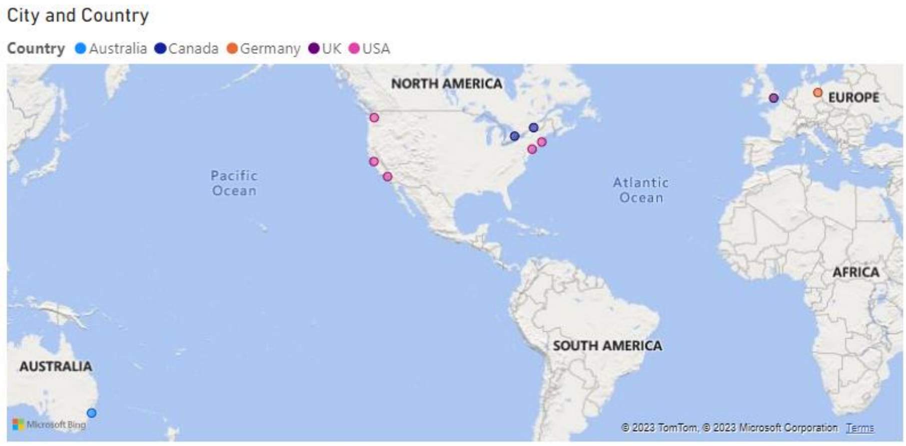
This dashboard constitutes of the country/city wise details of cyber-attacks on the organisation that had occurred during the year 2022. The organisation runs it operations across several countries. Along with the Time of attack, Industry affected, Threat Type, Attack Vector used and Target of the attack, it also highlights the severities of impact and the monetary losses the organisation had faced due to these attacks. It was observed that these attacks had occurred on the 1st of every month between January and October.

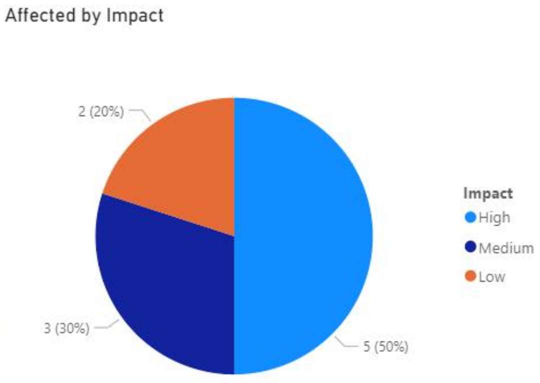
The **highest** impacted cities were Australia- Sydney, North America- New York, Seattle, Los Angeles, and Germany- Berlin. In **Sydney**, the Energy industry was impacted by Ransomware using a Malicious attachment. The attack's target was Operational Data and caused a loss of $3 million. In **New York**, the Final industry was impacted by Ransomware using a Phishing email. The attack was targeted on Financial Data and caused a loss of $2 million. In **Seattle**, the Hospitality industry was impacted by Advanced Persistent Threat using a Malicious link. The attack was targeted on Intellectual Property and caused a loss of $4 million. In **Berlin**, the Manufacturing industry was impacted by Advanced Persistent Threat using Spear Phishing. The attack was targeted on Intellectual Property and caused a loss of $5 million. In **Los Angeles**, the Retail industry was impacted by Social Engineering threat using Phone Calls. The attack was targeted on Customer Data and caused a loss of $1.5 million.

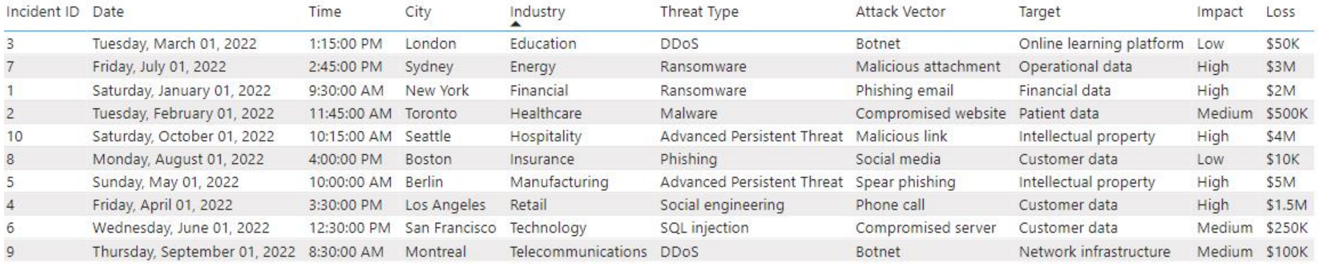
Moderately impacted cities were United States- San Francisco, Canada- Toronto, Montreal. In **San Francisco**, the Technology industry was impacted by SQL Injection through a Compromised Server. The attack's target was Customer Data and caused a loss of $250,000. In **Toronto**, the Healthcare industry was impacted by Malware through a Compromised Website. The attack's target was Patient Data and caused a loss of $500,000. In **Montreal**, the Telecommunications industry was impacted by DDos through Botnet. The attack's target was Network Infrastructure and caused a loss of $100,000

The **least** impacted cities were United States- Boston and United Kingdom- London. In **Boston**, the Insurance industry was impacted by Phishing using Social Media. The attack's target was Customer Data and caused a loss of $10,000. In **London**, the Education industry was impacted by DDos using Botnet. The attack's target was an Online Learning Platform and caused a loss of $50,000.

P1 (Chart 1 and 2)



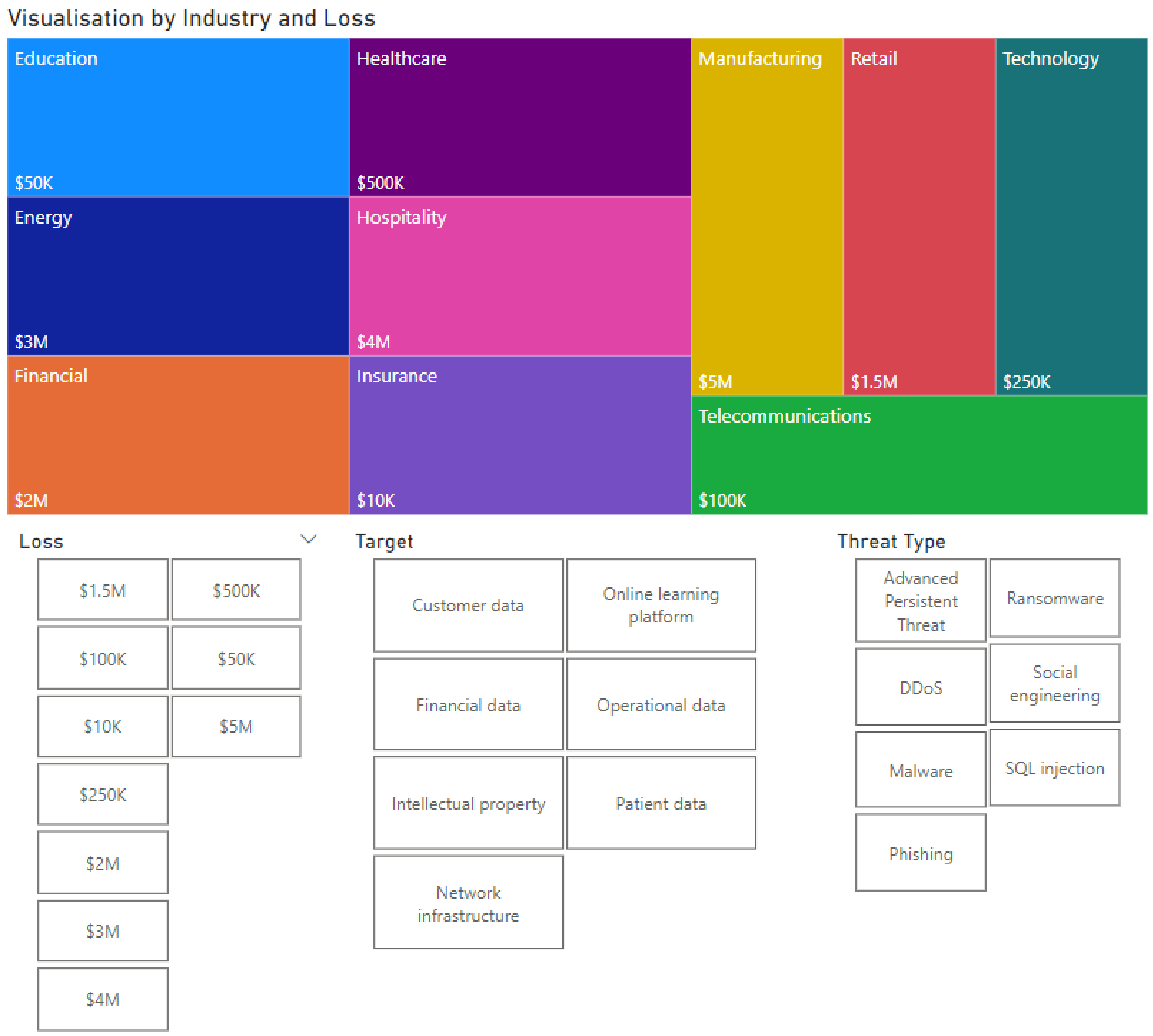




Incident ID	Date	Time	City	Industry	Threat Type	Attack Vector	Target	Impact	Loss
3	Tuesday, March 01, 2022	1:15:00 PM	London	Education	DDoS	Botnet	Online learning platform	Low	$50K
7	Friday, July 01, 2022	2:45:00 PM	Sydney	Energy	Ransomware	Malicious attachment	Operational data	High	$3M
1	Saturday, January 01, 2022	9:30:00 AM	New York	Financial	Ransomware	Phishing email	Financial data	High	$2M
2	Tuesday, February 01, 2022	11:45:00 AM	Toronto	Healthcare	Malware	Compromised website	Patient data	Medium	$500K
10	Saturday, October 01, 2022	10:15:00 AM	Seattle	Hospitality	Advanced Persistent Threat	Malicious link	Intellectual property	High	$4M
8	Monday, August 01, 2022	4:00:00 PM	Boston	Insurance	Phishing	Social media	Customer data	Low	$10K
5	Sunday, May 01, 2022	10:00:00 AM	Berlin	Manufacturing	Advanced Persistent Threat	Spear phishing	Intellectual property	High	$5M
4	Friday, April 01, 2022	3:30:00 PM	Los Angeles	Retail	Social engineering	Phone call	Customer data	High	$1.5M
6	Wednesday, June 01, 2022	12:30:00 PM	San Francisco	Technology	SQL injection	Compromised server	Customer data	Medium	$250K
9	Thursday, September 01, 2022	8:30:00 AM	Montreal	Telecommunications	DDoS	Botnet	Network infrastructure	Medium	$100K

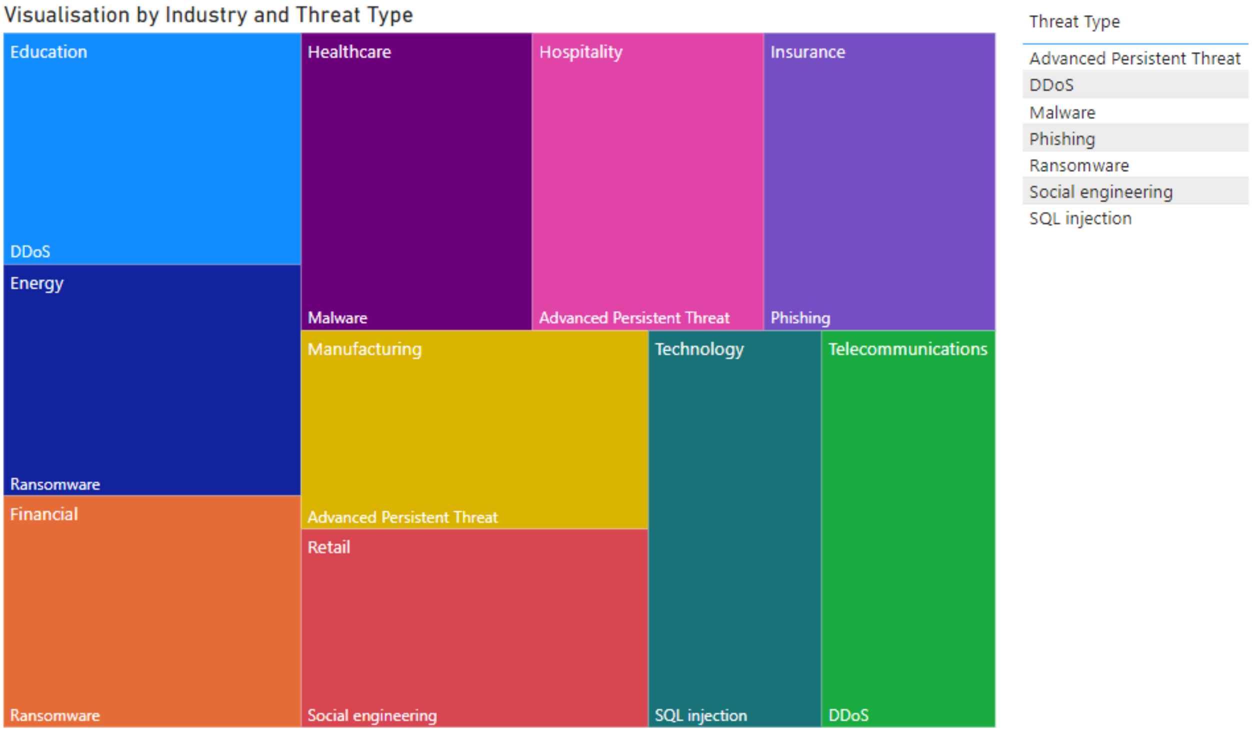
This page includes two charts: Map- to highlight the impacted locations, Pie Chart- to show the severity and impact percentage of the attacks, Table- to provide detailed insights about each attack. 50% of the cities were highly affected by the attacks and caused huge monetary losses. 30% of the cities were moderately affected by the attacks and caused considerable monetary losses. 20% of the cities were least affected by these attacks and caused least number of monetary losses. It was observed that highest number of affected cities were in the United States followed by Canada, Australia, Germany, and United Kingdom.

P2 (Chart 3)



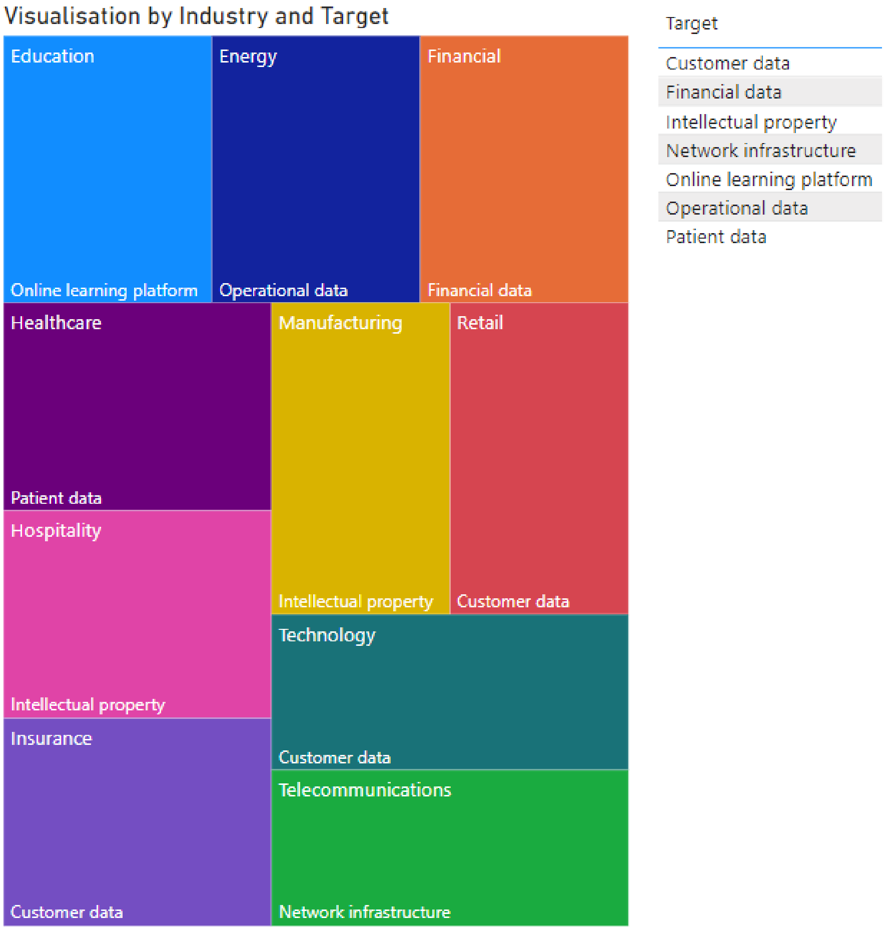
The Treemap is used to visualise monetary losses due to cyber-attacks faced by the organisation on the basis of different industries. Slicers have been added to provide interaction and more clarity on the Target and Threat Type involved in the losses. Manufacturing industry faced the highest monetary loss amounting to $5 million followed by the Hospitality industry which faced a loss of $4 million. Energy industry faced a loss of $3 million followed by the Financial industry which faced a loss of $2 million. Retail industry faced a loss of $1.5 million followed by the Healthcare industry which faced a loss of $500,000. Technology industry went through a loss of $250,000 followed by the Telecommunications industry which faced a loss of $100,000. Education industry faced a loss $50,000 followed by the Insurance industry which faced the least loss of $10,000.

P3 (Chart 4)



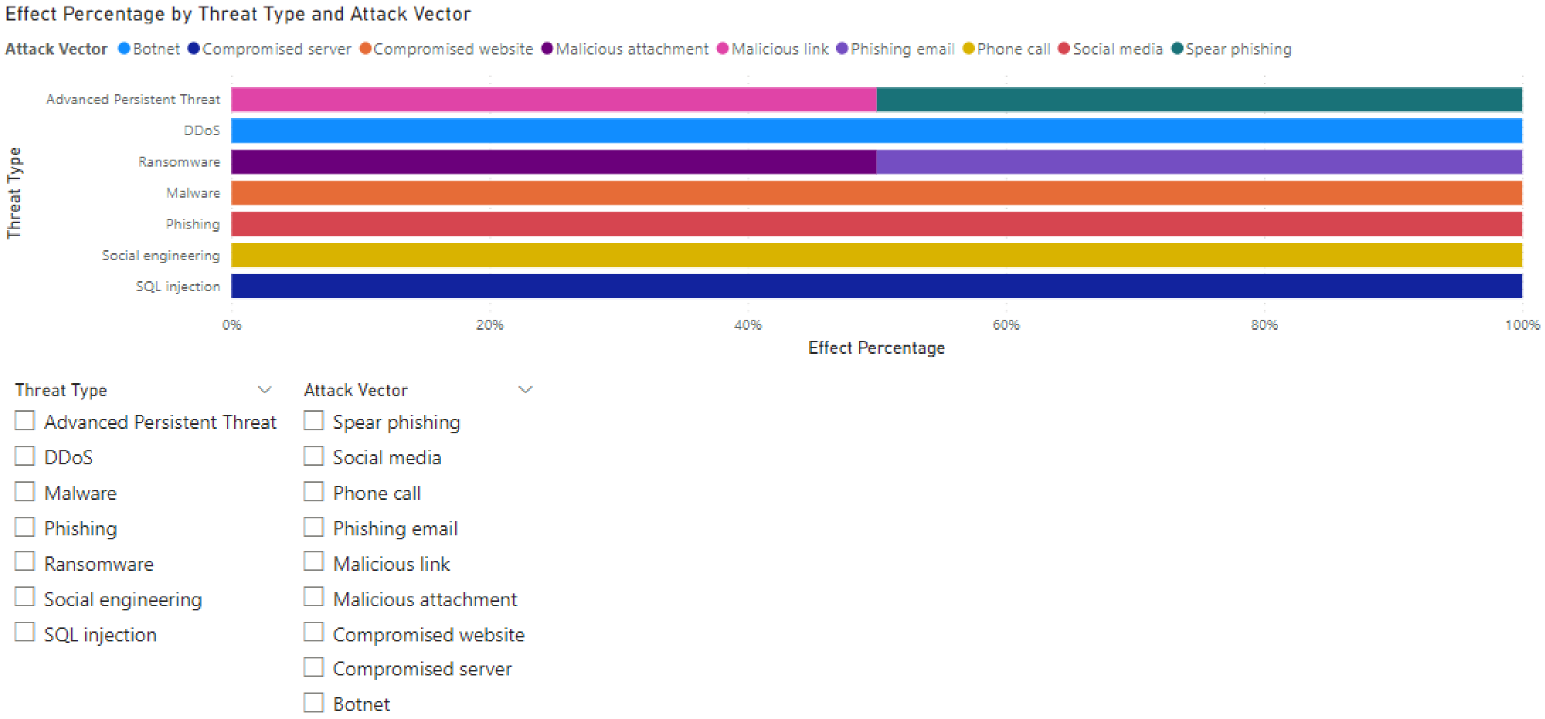
The Treemap is used to visualise different industries of the organisation on the basis of the attack's Threat Type. The table containing threat type has been added to provide better clarity and interaction. Industries affected- Education and Telecommunications were impacted by DDos, Healthcare by Malware, Hospitality and Manufacturing by Advanced Persistent Threat, Insurance by Phishing, Energy and Financial by Ransomware, Retail by Social Engineering, and Technology by SQL Injection.

P4 (Chart 5)



The Treemap is used to visualise different industries of the organisation on the basis of attack’s Target data. The Target table has been added to provide better clarity and interaction. Industries affected- Education industry was targeted to compromise their Online learning platform, Energy for their Operational Data, Financial for the Financial Data, Healthcare for their Patient Data, Manufacturing and Hospitality for their Intellectual Property. Retail, Insurance and Technology industries were targeted for their Customer Data whereas Telecommunications for their Network Infrastructure.

P5 (Chart 6)


Effect Percentage by Threat Type and Attack Vector
Attack Vector ● Botnet ● Compromised server ● Compromised website ● Malicious attachment ● Malicious link ● Phishing email ● Phone call ● Social media ● Spear phishing
Threat Type
Advanced Persistent Threat
DDoS
Ransomware
Malware
Phishing
Social engineering
SQL injection
0%
20%
40%
60%
80%
100%
Effect Percentage

Threat Type

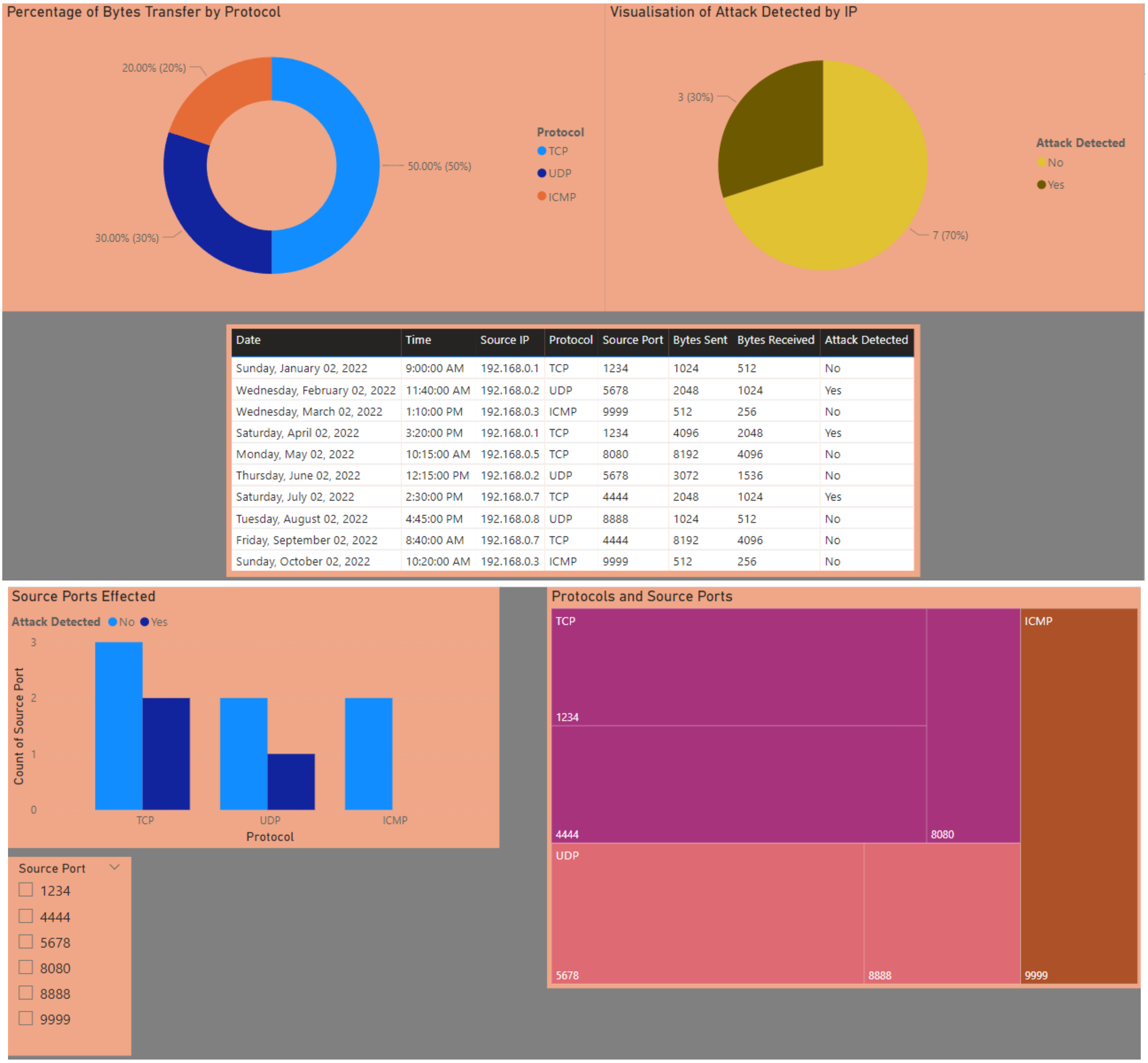
- ☐ Advanced Persistent Threat
- ☐ DDoS
- ☐ Malware
- ☐ Phishing
- ☐ Ransomware
- ☐ Social engineering
- ☐ SQL injection

Attack Vector

- ☐ Spear phishing
- ☐ Social media
- ☐ Phone call
- ☐ Phishing email
- ☐ Malicious link
- ☐ Malicious attachment
- ☐ Compromised website
- ☐ Compromised server
- ☐ Botnet

The 100% Stacked Bar Chart has been utilised to show the percentage effect caused by the attack on the basis of Threat Type and Attack Vector. The slicers have been inserted to deliver better interaction and clarity. Threat Types and Attack Vectors: Advanced Persistent Threat- Use of Malicious Link and Spear Phishing contributed by 50% each. DDos- Use of Botnet contributed by 100%. Ransomware- Use of Malicious Attachment and Phishing Email contributed by 50% each. Malware- Use of Compromised Website contributed by 100%. Phishing- Use of Social Media contributed by 100%. Social Engineering- Use of Phone Calls contributed by 100%. SQL Injection- Use of Compromised Server contributed by 100%.

2.3 Network Traffic Data Dashboard for the Network Administrator



Date	Time	Source IP	Protocol	Source Port	Bytes Sent	Bytes Received	Attack Detected
Sunday, January 02, 2022	9:00:00 AM	192.168.0.1	TCP	1234	1024	512	No
Wednesday, February 02, 2022	11:40:00 AM	192.168.0.2	UDP	5678	2048	1024	Yes
Wednesday, March 02, 2022	1:10:00 PM	192.168.0.3	ICMP	9999	512	256	No
Saturday, April 02, 2022	3:20:00 PM	192.168.0.1	TCP	1234	4096	2048	Yes
Monday, May 02, 2022	10:15:00 AM	192.168.0.5	TCP	8080	8192	4096	No
Thursday, June 02, 2022	12:15:00 PM	192.168.0.2	UDP	5678	3072	1536	No
Saturday, July 02, 2022	2:30:00 PM	192.168.0.7	TCP	4444	2048	1024	Yes
Tuesday, August 02, 2022	4:45:00 PM	192.168.0.8	UDP	8888	1024	512	No
Friday, September 02, 2022	8:40:00 AM	192.168.0.7	TCP	4444	8192	4096	No
Sunday, October 02, 2022	10:20:00 AM	192.168.0.3	ICMP	9999	512	256	No

Source Port

☐ 1234
☐ 4444
☐ 5678
☐ 8080
☐ 8888
☐ 9999

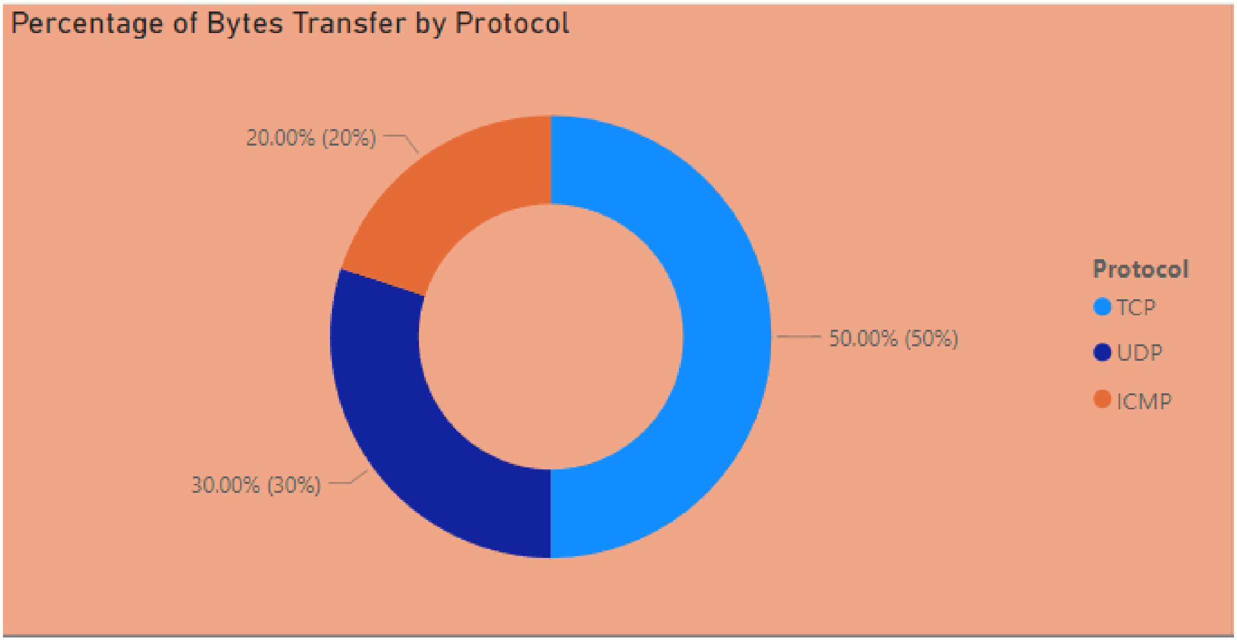
This dashboard represents the information regarding a company's computer system data interaction within the local network as well as with the outside world. The data is from the 2nd of every month between January and October from the year 2022. Besides providing information about the Time of suspicious interaction, Source IP, Source Port and bytes exchanged, it also highlights different Protocols involved in the data interaction. This dashboard makes it easier to identify whether a particular data exchange involved any Cyber Attack or not. A table has been added to provide better interaction and shed more transparency about the data.

In the 50% of data exchanged using TCP, 20% of it was affected by an attack whereas 30% of it was unaffected. The affected Source IP addresses were 192.168.0.1 and 192.168.0.7. Using 192.168.0.1 and source port 1234 on April 2nd, 4096 bytes were sent, and 2048 bytes were received. Using 192.168.0.7 and source port 4444 on July 2nd, 2048 bytes were sent, and 1024 bytes were received.

In the 30% of data exchanged using UDP, 10% of it was affected by an attack whereas 20% of it was unaffected. The affected Source IP address was 192.168.0.2. Using 192.168.0.2 and source port 5678 on February 2nd, 2048 bytes were sent, and 1024 bytes were received.

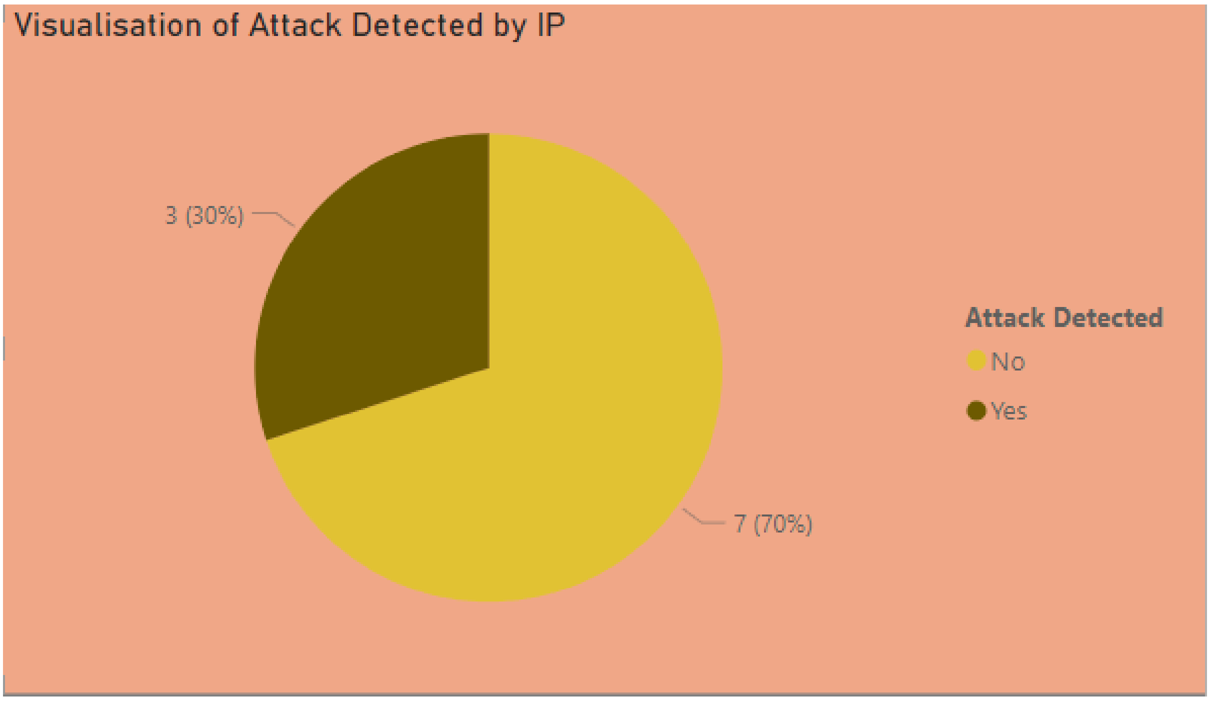
In the 20% of data exchanged using ICMP, none of it was affected by an attack.

Chart 1



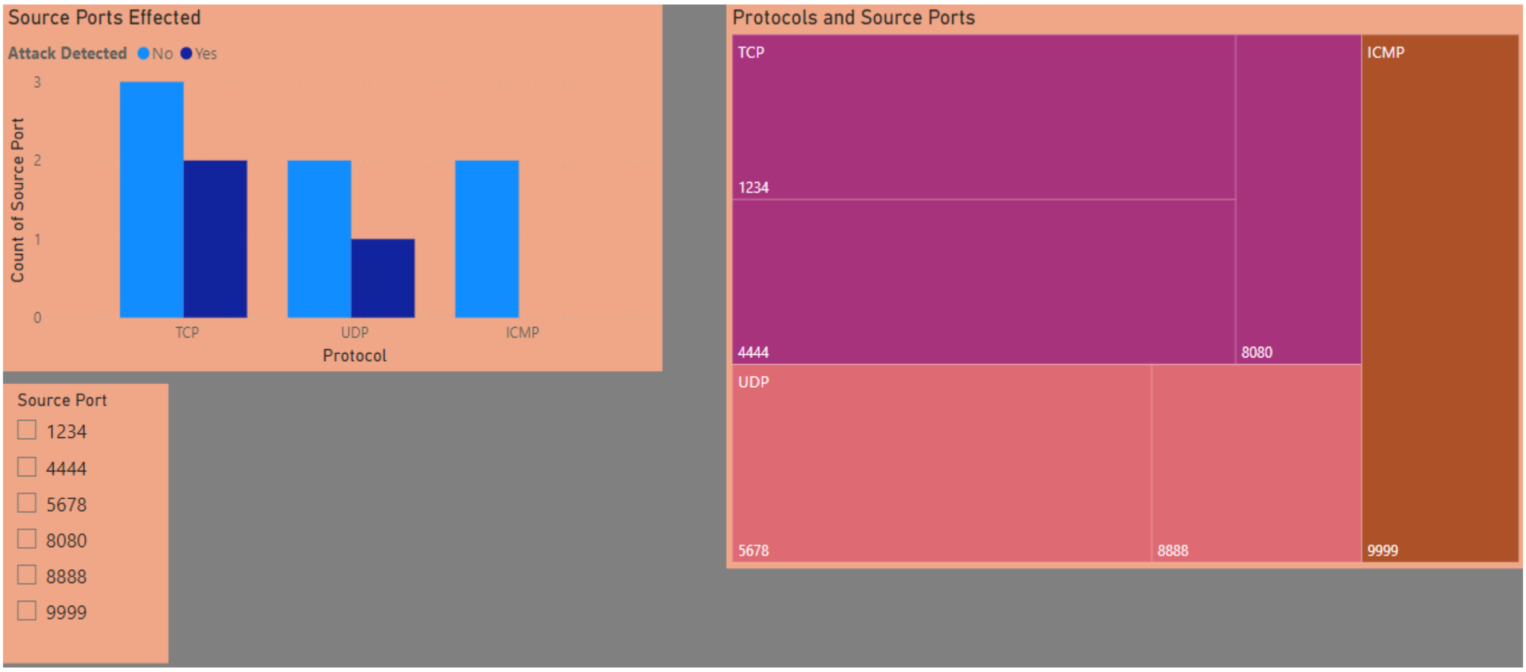
This donut represents the protocols involved and their contribution percentage in bytes transfer. TCP was the most used protocol and was involved in the exchange of 50% of the data followed by UDP which was involved in the exchange of 30% of the data. ICMP was the least used protocol and was involved in the exchange of 20% of the data.

Chart 2



This pie chart appropriately represents whether the data exchange involved any cyber-attack or not. 30% of the data interaction involved being impacted by a cyber-attack whereas 70% of the data interaction was not.

Chart 3 and Chart 4



This **clustered column chart** represents the number of source ports involved in data exchange on the basis of the protocols used and whether an attack was involved or not. Source ports using TCP- Two ports were impacted by an attack whereas 3 were not. Source ports using UDP- One port was impacted by an attack whereas 2 were not. Source ports using

ICMP- Two ports were used and neither of them involved any attack. TCP was the highest impacted whereas ICMP was the least impacted protocol.

The **slicer** has been added to be used commonly for both charts. It aims to provides clarity and better interaction among the charts.

The **Treemap** has been utilised to represent the protocols involved in the data exchange but on the basis of the precise source port numbers that were involved. TCP used the source ports 1234, 4444, and 8080. UDP used the source ports 5678 and 8888. ICMP used the source port 9999. TCP used the highest (3) number of source ports whereas ICMP used only 1.

3. Recommendations

Dashboard 1: Sales of the company's cyber security products is low in the Europe and North America region. The overall highest performing products were Endpoint Security, Cloud Security, and Network Security. These are being sold only in the Asia Pacific region. To increase the sales in the other two regions, it is recommended that the company must introduce these 3 products and focus on its marketing campaigns.

Dashboard 2: The organisation faced huge monetary losses and was majorly impacted by:

- Ransomware using Malicious attachment and Phishing email.
- Advanced Persistent Threat using Malicious Link and Spear Phishing.
- Social Engineering using Phone calls.

It is recommended to take up preventive measures such as having weekly townhall meetings highlighting the importance of Cyber Security, types of attacks and practices to follow in order to avoid those should be conducted. Based on these points and on a regular basis, specific emails must be sent out to all the employees in order to increase the awareness. Gearing up the security infrastructure to be immune to such attacks will also be beneficial.

Dashboard 3: TCP was the highest attack-impacted protocol involved in data exchange whereas ICMP was the least impacted. To be less prone to cyber-attacks, it is recommended that the company should be open to switching to ICMP or other safe protocols when it is the need of the hour. Amping up the security measures of the Network Infrastructure will be a major contributor towards avoiding cyber-attacks.

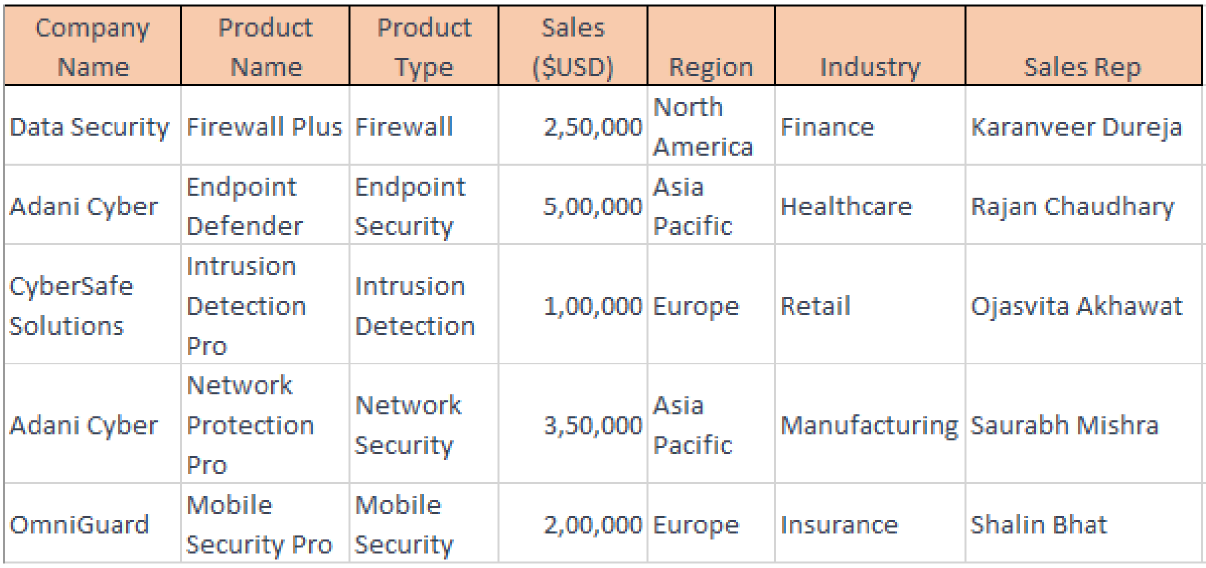
4. References

1. *What is an Attack Vector? Common Attack Vectors*. (n.d.). Www.upguard.com. https://www.upguard.com/blog/attack-vector
2. *What are the differences between TCP, UDP, and ICMP packet types? | PingPlotter*. (n.d.). Www.pingplotter.com. https://www.pingplotter.com/wisdom/article/packet-type-differences
3. *What is Cybersecurity*. (n.d.). Check Point Software. https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cybersecurity/

5. Appendix

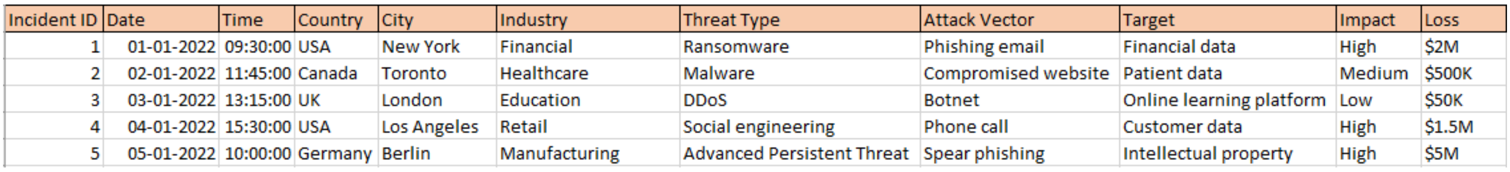
Datasets formed and Used:

1. Cyber Security Sales Data



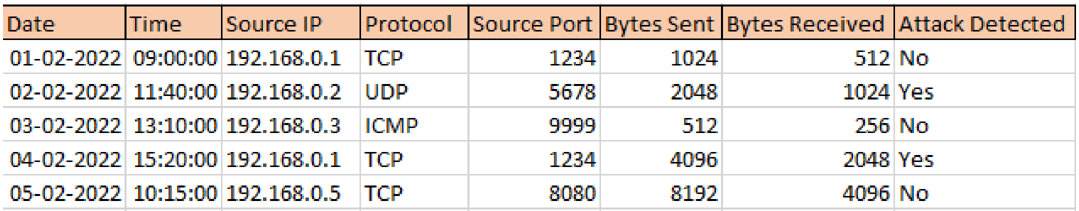
Company Name	Product Name	Product Type	Sales ($USD)	Region	Industry	Sales Rep
Data Security	Firewall Plus	Firewall	2,50,000	North America	Finance	Karanveer Dureja
Adani Cyber	Endpoint Defender	Endpoint Security	5,00,000	Asia Pacific	Healthcare	Rajan Chaudhary
CyberSafe Solutions	Intrusion Detection Pro	Intrusion Detection	1,00,000	Europe	Retail	Ojasvita Akhawat
Adani Cyber	Network Protection Pro	Network Security	3,50,000	Asia Pacific	Manufacturing	Saurabh Mishra
OmniGuard	Mobile Security Pro	Mobile Security	2,00,000	Europe	Insurance	Shalin Bhat

2. Cyber Security Incidents Data



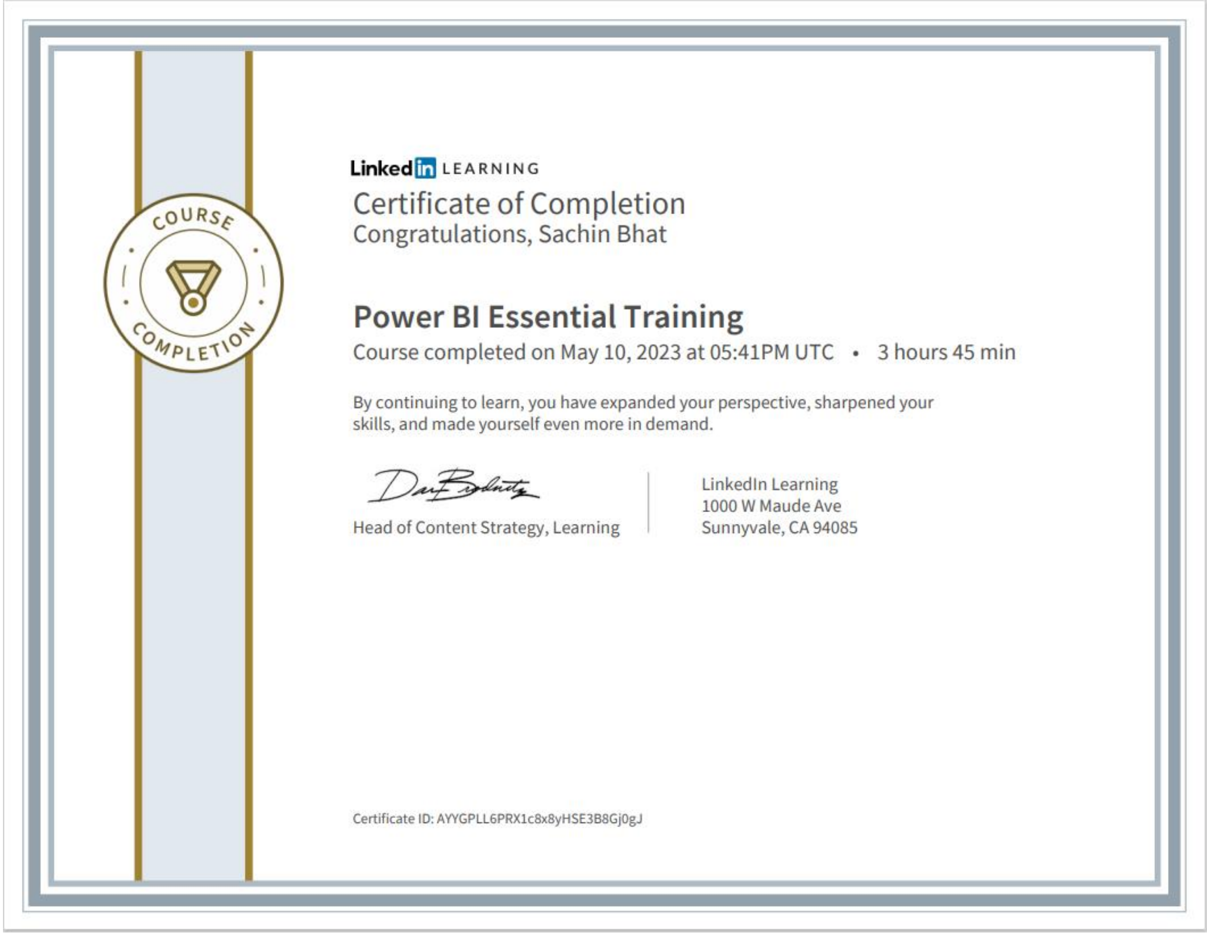
Incident ID	Date	Time	Country	City	Industry	Threat Type	Attack Vector	Target	Impact	Loss
1	01-01-2022	09:30:00	USA	New York	Financial	Ransomware	Phishing email	Financial data	High	$2M
2	02-01-2022	11:45:00	Canada	Toronto	Healthcare	Malware	Compromised website	Patient data	Medium	$500K
3	03-01-2022	13:15:00	UK	London	Education	DDoS	Botnet	Online learning platform	Low	$50K
4	04-01-2022	15:30:00	USA	Los Angeles	Retail	Social engineering	Phone call	Customer data	High	$1.5M
5	05-01-2022	10:00:00	Germany	Berlin	Manufacturing	Advanced Persistent Threat	Spear phishing	Intellectual property	High	$5M

3. Network Traffic Data



Date	Time	Source IP	Protocol	Source Port	Bytes Sent	Bytes Received	Attack Detected
01-02-2022	09:00:00	192.168.0.1	TCP	1234	1024	512	No
02-02-2022	11:40:00	192.168.0.2	UDP	5678	2048	1024	Yes
03-02-2022	13:10:00	192.168.0.3	ICMP	9999	512	256	No
04-02-2022	15:20:00	192.168.0.1	TCP	1234	4096	2048	Yes
05-02-2022	10:15:00	192.168.0.5	TCP	8080	8192	4096	No

Certificate of Power BI Course Completion:



COURSE
COMPLETION

Linked in LEARNING

Certificate of Completion

Congratulations, Sachin Bhat

Power BI Essential Training

Course completed on May 10, 2023 at 05:41PM UTC • 3 hours 45 min

By continuing to learn, you have expanded your perspective, sharpened your skills, and made yourself even more in demand.

Head of Content Strategy, Learning

LinkedIn Learning
1000 W Maude Ave
Sunnyvale, CA 94085

Certificate ID: AYYGPLL6PRX1c8x8yHSE3B8Gj0gJ