CommonWealth

Introduction to CyberSecurity

Manasvi Sagathiya
Milind Bhonsale
Durga Bhavani

Project Overview

The goal of this project is to improve cybersecurity for financial systems by analyzing vulnerabilities, responding to incidents, raising security awareness, and testing system defenses.

- Data Analysis
- Incident Response
- Security Awareness
- Penetration Testing

Project Timeline

Task 1	Task 2	Task 3	Task 4
Data Analysis	Incidence Response	Security Awareness	Pen Testing
Duration: 2 weeks	**Duration:** 1 week	**Duration**: 2 weeks	**Duration**: 3 weeks

Task 1

Data Analysis using Splunk

Executive Summary:
The cybersecurity team at Commonwealth Bank is leveraging Splunk to build a data-driven dashboard that enhances fraud detection and help us in the identification of suspicious activities, trends, and anomalies.

Task 1

Approach

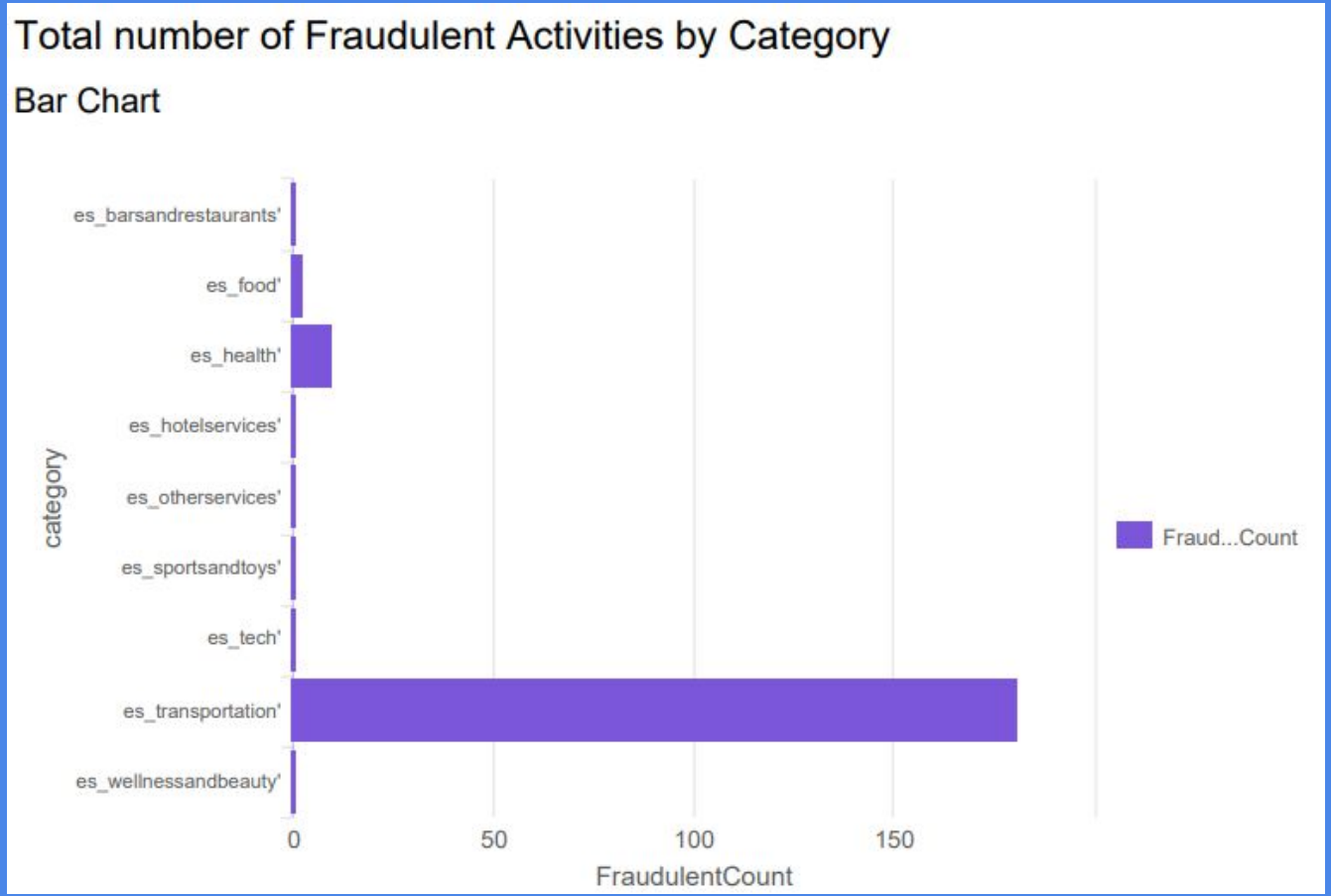
The approach focused on leveraging data visualization to transform datasets into clear, actionable insights. Key steps included:

1. Integrating and analyzing financial transaction data.
2. Building interactive visualizations to identify patterns and anomalies.
3. Establishing metrics to monitor suspicious activities in real time.

Results

1. Improved Detection: Enabled rapid identification of fraudulent patterns and trends.
2. Actionable Insights: Provided clear visualizations for efficient decision-making.
3. Enhanced Response: Reduced response time to potential fraud cases.
4. Operational Efficiency: Strengthened monitoring with real-time metrics and reports.

Task 1

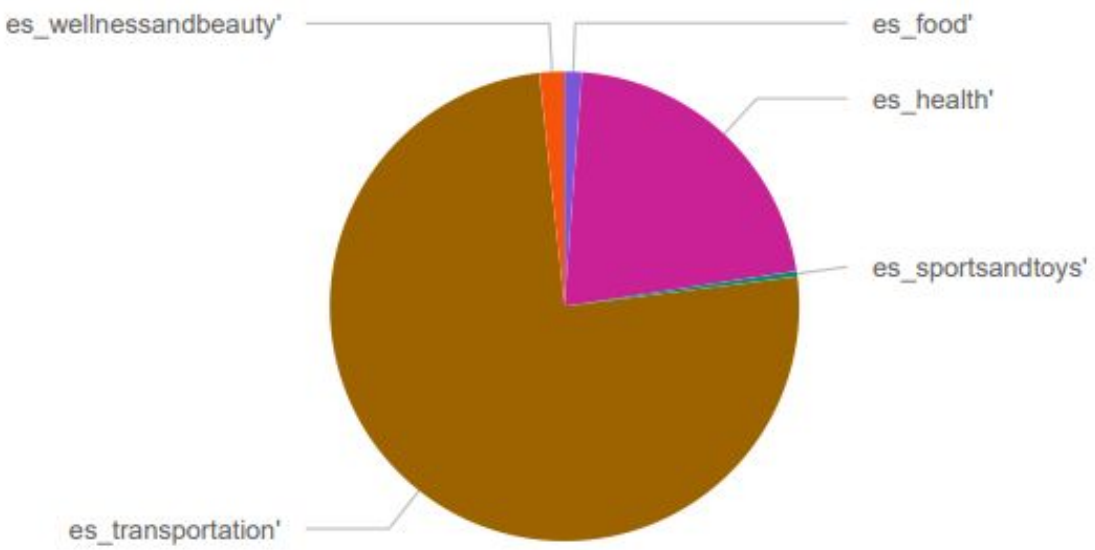


Task 1

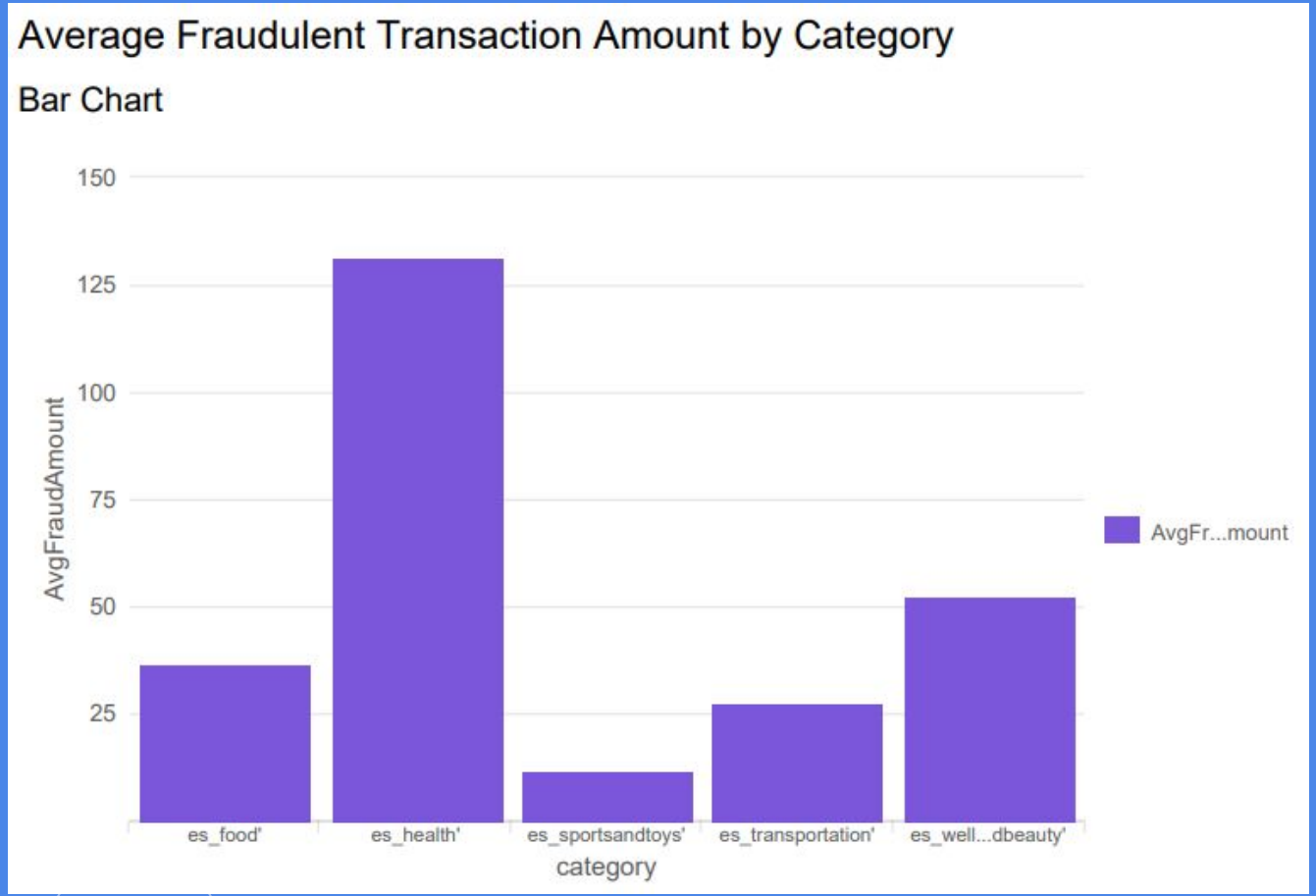
7

Total Fraudulent Transactions Amount by Category

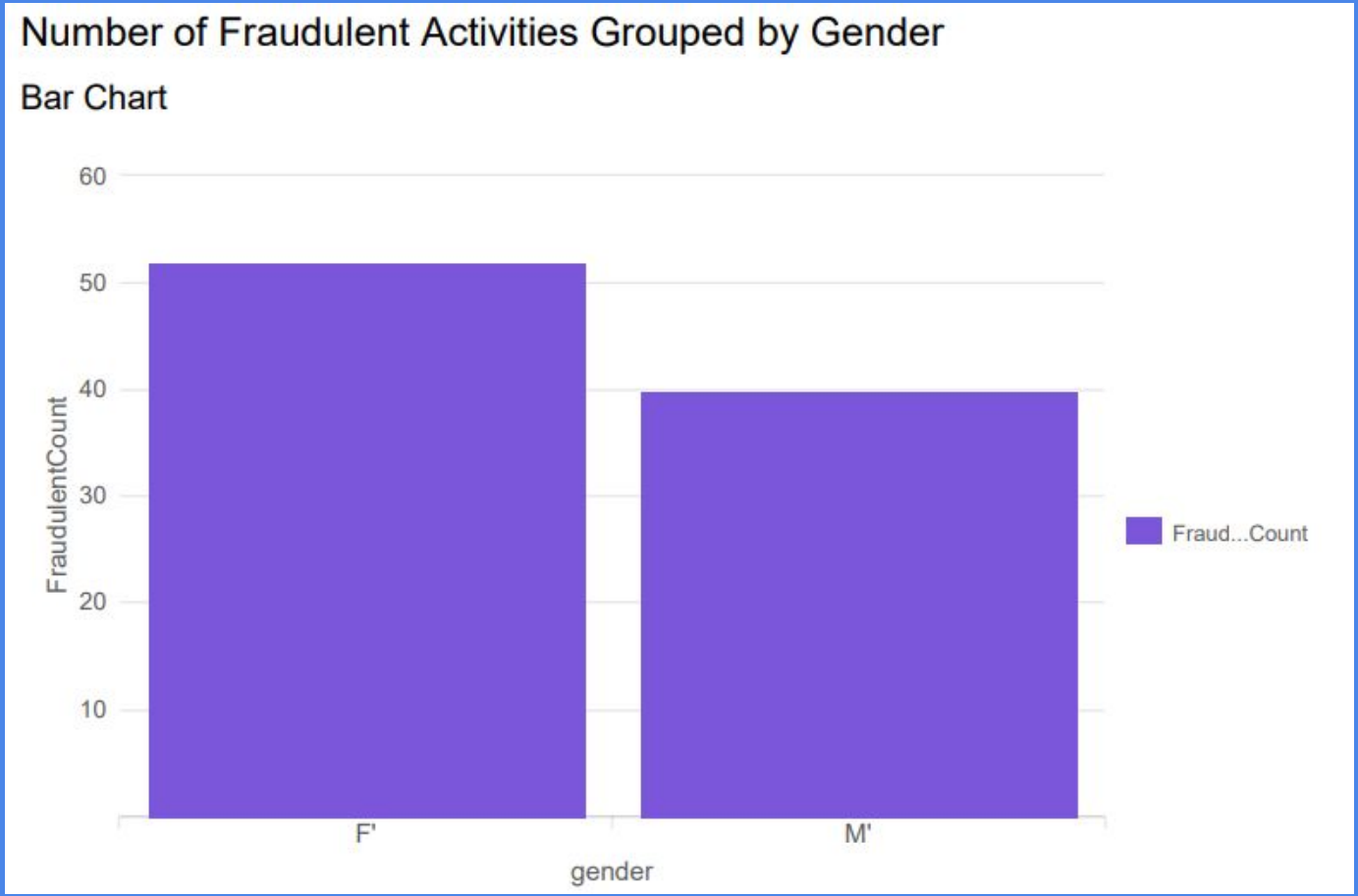
Pie Chart



Task 1



Task 1



Task 1

10

Health Category

step	customer	age	gender	postcoc	mercha	category	amount	fraud
1	C583110837'	2	M'	28007'	M4801390	es_health'	44.26	1
1	C1332295774'	2	M'	28007'	M4801390	es_health'	324.5	1
1	C274486575'	1	F'	28007'	M6928985	es_health'	171.07	1
2	C1817842389'	4	M'	28007'	M6928985	es_health'	109.26	1
3	C1463833315'	0	M'	28007'	M1053599	es_health'	7.94	1

Transportation Category

step	customer	age	gender	postcoc	mercha	category	amount	fraud
0	C2054744914'	3	F'	28007'	M1823072	es_transportation'	26.89	1
0	C757503768'	4	M'	28007'	M3489346	es_transportation'	35.72	1
0	C1315400589'	2	F'	28007'	M3489346	es_transportation'	25.81	1
0	C765155274'	0	F'	28007'	M3489346	es_transportation'	9.1	1
0	C98707741'	1	F'	28007'	M3489346	es_transportation'	14.95	1
0	C1865204568'	4	M'	28007'	M1823072	es_transportation'	20.32	1
0	C1207205377'	3	M'	28007'	M1823072	es_transportation'	17.54	1
0	C124539163'	1	F'	28007'	M3489346	es_transportation'	10.09	1
0	C1687101094'	1	F'	28007'	M3489346	es_transportation'	19.31	1
0	C1622124632'	1	M'	28007'	M3489346	es_transportation'	29.84	1
0	C1563705147'	4	F'	28007'	M3489346	es_transportation'	32.27	1
0	C998987490'	1	F'	28007'	M3489346	es_transportation'	32.7	1

Task 1

Challenges Encountered

- **Learning Splunk:** Gaining expertise in Splunk's tools and functionalities posed an initial learning curve.
- **Efficient Data Usage:** Structuring and optimizing large datasets for meaningful analysis and actionable insights.
- **Clear Visualizations:** Creating concise, intuitive, and impactful dashboards.

Summary

By implementing a Splunk-based dashboard, the team significantly improved Commonwealth Bank’s ability to detect, mitigate, and prevent financial fraud.

This initiative not only protects customer assets and the bank’s reputation but also enhances the resilience of its financial systems against evolving fraud tactics.

Task 2: Cybersecurity Incident Management and Recovery Actions

Threat Identification: System logs analysis and reports to identify the exact type of attack, be it phishing or ransomware.

Immediate Actions: Isolate the affected systems, secure backup data, and quickly notify the incident response team.

Containment and Eradication: Eliminate malware, reinstate compromised systems, and confirm that the threat has been eliminated.

Recovery and Monitoring: Restore lost data, validate system functionality, and monitor for signs of recurring issues.

Post-Incident Improvement: Review security protocols, further training for staff, and the use of more effective protective measures.

Summary

Management of cybersecurity incidents would therefore include establishing the nature of the attack, whether phishing or ransomware, through system logs and reports.

It immediately takes actions to isolate the affected systems, secures backups, and notifies the response team for mitigation.

Containment and eradication involve thorough threat removal, restoration of systems and data, and monitoring for recurrence.

Post-event enhancements have focused on the updating of security protocols, training of staff, and stronger preventive measures.

Challenges:

Complex Threats: Difficulty in identifying sophisticated attacks like phishing and ransomware.

Response Time: This needs quick action to minimize damage and data loss.

System Restoration: Ensuring systems are fully restored without any residual threats.

Continuous Monitoring: Identification and addressing of recurring vulnerabilities or attacks.

Results:

Swift Incident Resolution: Effective containment and elimination of cybersecurity threats minimized damage and disruption.

Data Integrity Restoration: The successful recovery of lost or compromised data ensured business continuity.

Improved System Security: Enhanced defenses reduced the chances of similar attacks in the future.

Better Staff Preparedness: Training and awareness programs help employees identify the threat and respond accordingly.

Task 3

Security Awareness Knowledge

Task 4

Penetration Testing

Executive Summary:
This report evaluates the vulnerabilities and security gaps of the Basic Mission challenges of Hack This Site. The purpose was to simulate common security issues faced by web applications, such as weak authentication, improper input validation, and exposed sensitive files.

Mission	Vulnerability	Approach	Recommendation
Authentication Bypass (The Idiot Test)	Exposed HTML comments.	Right-click anywhere on the web page, choose view page source. Scroll down until we find the word password or Ctrl + f and type the word password.	Passwords should never be stored in plaintext in the source code. We can store it as a hashed value in a separate file or kept in an encrypted file. Hashing is more secure.
Directory Traversal	Improper File handling	Leave the password button blank and click submit.	Always test the application by submitting an empty blank password field.
Hardcoded Password	Static password embedded in the page source.	Right-click anywhere on the web page, choose view page source. On the hidden form, the value is password.php. So, please visit https://www.hackthissite.org/missions/basic/3/password.ph.	Map out the directory structure of a web application before deploying it.

Email Password	he wrote a script that would email his password to him automatically in case he forgot	Right-click anywhere on the web page, choose view page source. On the type: hidden input, the value should be changed from sam@hackthissite.org to whatever email address corresponds to your account.	Sensitive information should not be included in the code if it is carried out on the client-side. Protect the sensitive information from being accessed by unauthorized personnels.
Hidden Email	Hiding email but still recoverable using Inspect	Right-click anywhere on the web page, choose view page source. On the type: hidden input, the value should be changed from sam@hackthissite.org to whatever email address corresponds to your account.	Sensitive information should not be included in the code if it is carried out on the client-side. Protect the sensitive information from being accessed by unauthorized personnels.
Basic Cryptanalysis	Weak encryption algorithm	Decrypted a base64-encoded string to retrieve credentials.	Use stronger encryption algorithms for sensitive data

Mission	Vulnerability	Approach	Mitigation
UNIX cal command	Straight away Script execution	The web app is using a script (Perl) that includes number the user input and shows a calendar for the specific year on the website. The command "is cal -y" (Year). We exploit this by typing ;ls on the view form box (command injection). We found k1kh31b1n55h.php and placed it on the web browser search page (Just put it at the bank of the link). Then we found the password.	Sanitise the user input before executing on the web application.
PHP File	Incomplete Security knowledge	<!--#exec cmd="ls ../" -->	Validate access rights on the server side

The Hidden Approach	Javascript Vulnerability	This is incorrect implementation of cookies. Anyone can hijack the session but changing the authorization mode. Click Developer tool and navigate to console. Run this command document.cookie. When it is done, enter and run this command document.cookie="level10_authorized=yes";. Alternatively, on the Developer tool, please navigate to Application. On the value column of level10_authorized, change the value from no to yes.	Do not use yes/no cookies for authentication as it will store a session ID that is associated with the authentication of the user on the server side. This will allow the server to grant access to user without the password.
Directory	Weak session handling.	.htaccess DaAnswer/ It says that the answer is around	Learn Apache. Configure Apache web server to make sure not everyone can read the configuration of web server. The directory DaAnswer should not be made public otherwise it could be exploited. Correct the file permission, implement authentication and access control.

Challenges

- Lot of brainstorming
- Research
- Had to learn Javascript, Perl
- Encryption/Decryption

Result

- Successfully implemented all the tasks
- Learn a lot about Cybersecurity world

GROUP - 6

Peace out