

CyberSentinel

Sprint 2 By Team Tech Titans

Agenda

01

Team & Planning

- Team Roles & Responsibilities
- Improvements Based on Professor Feedback
- Project Description
- Team Working Agreement

04

Project Documentation & Management

- Sprint 1 Recap
- Diagrams
- Product Backlog
- Sprint 2 Backlog

02

User & Product Definition

- Personas
- Minimum Viable Product (MVP)

05

Tracking & Evaluation

- Metrics & Progress Tracking
- Sprint 2 Retrospective
- Sprint 3 Planning

03

Technology & Implementation

- Technologies
- Algorithms

06

Demonstrations & Resources

- Project Demo - Sprint 2
- GitHub Repository Link
- Live Application Demo



Team Members



Vaishnavi Dasari

Machine learning Engineer



Snehitha Bodiga

Full Stack Developer



**Aasritha
Bhimisetty**

Frontend Developer

Team Members



Abisainath

Backend Developer



Shoib Khan Patan **Dhanush Kolapalli**

Backend Developer

Machine Learning Engineer



Team Members



Neelkamal Rana

Full Stack Developer





Improvements



- Core details for MVP
 - Removal of Feature Column in US.
 - Adding API Slide
 - Test Case ID
- 

+++

Project Description

Project Name:	CyberSentinel
Team:	Tech Titans
Project Description:	<p>For individuals and enterprises who need protection against cyber threats, the CyberSentinel platform is a real-time AI-driven cybersecurity solution that detects and prevents phishing attacks, fraudulent transactions, and identity theft using advanced machine learning, behavioral analytics, and cloud-based threat intelligence.</p> <p>Unlike traditional security measures that struggle to detect sophisticated attack vectors, our application employs AI-powered risk assessment, real-time email scrutiny, transactional anomaly detection, and intelligent web link verification—continuously adapting to emerging threats to provide proactive and highly sophisticated cybersecurity defenses.</p>
Benefit Outcomes:	<ul style="list-style-type: none">Real-time detection and prevention of cyber threats, including phishing and fraudulent transactions.Adaptive learning capabilities to counter evolving attack techniques.Seamless integration of automation and analytics for efficient and proactive cybersecurity.User-friendly and intuitive design, making cybersecurity accessible for individuals and businesses.
Github Link:	https://github.com/htmw/2025S-Tech-Titans/wiki



Team Agreement

TEAM AGREEMENT

Communication:

- The team will use **Zoom** and **WhatsApp** as primary communication channels.
- **Google Docs** will serve as a platform for collaborative document editing, resource sharing, and note-taking during discussions.
- **Weekly Zoom meetings** will be scheduled to review progress, discuss roadblocks, and align on next steps. Additional meetings may be scheduled as needed.
- Team members should inform the group in advance if they are unable to attend a scheduled Zoom meeting.
- Regular updates on task progress are expected, and any challenges or delays should be promptly communicated to the team.
- Active participation is encouraged, with members providing constructive feedback and support when necessary.
- Discussions should be **focused**, with members listening attentively, speaking clearly, and staying on topic to prevent misunderstandings.
- All assigned work must be completed before the deadline. If any difficulties arise, members should reach out for assistance as early as possible to prevent disruptions to the project timeline.

Professionalism:

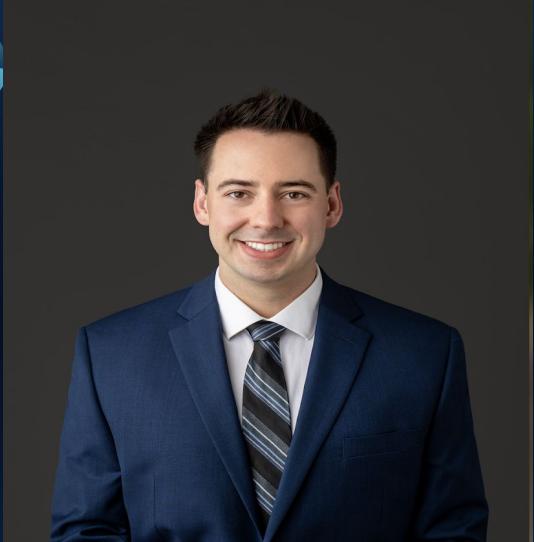
- Team interactions will be conducted with **mutual respect**, valuing diverse perspectives and contributions.
- Feedback should remain **constructive**, focusing on the project rather than personal attributes.
- If a team member disagrees with a decision, they may request a discussion in the next meeting for reconsideration.
- The team strives to maintain an **inclusive and supportive environment** where all members feel comfortable expressing their ideas.
- Any conflicts should be addressed **respectfully and transparently** within the team. If an agreement cannot be reached internally, the matter will be escalated to the professor for guidance.

Meeting Cadence:

- **Primary Meeting:** Weekly Zoom meeting to discuss progress, challenges, and next steps.
- **Check-ins:** Mid-week asynchronous updates via WhatsApp to ensure task alignment.
- **Ad-hoc Meetings:** Additional meetings scheduled as needed for urgent discussions or blockers.

Team Members:

- **Dasari Vaishnavi**
- **Snehittha Bodiga**
- **Arepalli Abisainath Reddy**
- **Shoaib Khan Patan**
- **Aasritha Bhimisetty**
- **Kolapalli Dhanush**
- **Rana Neelkamal**



Name: Alex Johnson

Age: 32

Occupation: Software Developer

Persona

Alex works at a mid-sized tech company and is well-versed in various technologies. Spends considerable time online, both professionally and personally. Aware of cybersecurity threats but seeks advanced tools to enhance personal security.

Goals:

- Protect personal and professional data from phishing and other cyber threats.
- Stay informed about the latest cybersecurity practices.
- Utilize AI-driven solutions for proactive threat detection.

Challenges:

- Balancing convenience with robust security measures.
- Identifying trustworthy cybersecurity tools amidst numerous options.



Name: Maria Thompson

Age: 40

Occupation: Project Manager

Persona

Manages a team remotely for a marketing firm. Juggles professional responsibilities with parenting two teenagers. Uses multiple devices for work and personal tasks.

Goals:

- Ensure the security of sensitive work-related information.
- Protect family members, especially children, from online threats.
- Maintain a secure digital environment across all devices.

Challenges:

- Limited time to manage and monitor cybersecurity measures.
- Keeping up with evolving cyber threats and ensuring family compliance with best practices.



Persona



Name: David Kim

Age: 45

Occupation: Owner of a local retail store

Runs an online storefront in addition to the physical store. Handles customer data, including payment information. Has basic knowledge of cybersecurity but lacks specialized expertise.

Goals:

- Protect customer data to maintain trust and comply with regulations.
- Prevent financial losses due to cyber attacks.
- Implement cost-effective security solutions without extensive technical knowledge.

Challenges:

- Limited budget for cybersecurity investments.
- Difficulty in assessing which security measures are necessary and effective.

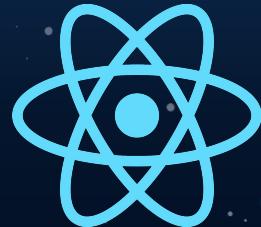
Minimum Viable Product (MVP)

- **Phishing Email Detection**
Uses NLP models trained on cybersecurity datasets to classify emails as safe or phishing. Helps prevent social engineering attacks by identifying malicious content in real-time.
- **Fraudulent Transaction Detection**
Applies anomaly detection techniques to flag suspicious financial transactions. This component supports real-time monitoring for enterprise-level financial systems.
- **URL Classification**
Analyzes lexical features of URLs to determine if a web link is malicious or safe. Provides an added layer of protection against phishing websites and drive-by downloads.
- **User Dashboard**
A centralized interface that displays alerts, threat levels, and risk analysis in real-time. It allows users to monitor cybersecurity threats and take quick preventive action.

+++

Technologies - Development Stack

- **Frontend:** React.js (for simple and interactive UI)
- **Backend:** Flask (lightweight Python-based API)
- **Database:** PostgreSQL (to store detected threat data)
- **Hosting:** AWS (for cloud deployment and scalability)



+++

Technologies - AI & Cybersecurity Tools

- **Machine Learning:** Scikit-learn, PyTorch
(for phishing and fraud detection)
- **Security:** OAuth 2.0 (for authentication),
OpenCV (for URL analysis)
- **Threat Detection Models:** NLP-based
phishing email classification, anomaly
detection for fraudulent transactions,
and URL classification algorithms



Algorithms

Phishing Email Detection:

Algorithm: BERT (Bidirectional Encoder Representations from Transformers)

- Utilizes a **pre-trained deep learning model** for text classification.
- **Captures contextual meaning** of words, improving phishing email detection.
- **Fine-tuned** on phishing email datasets for high accuracy.

Fraudulent Transaction Detection:

Algorithm: Autoencoder with Isolation Forest

- **Autoencoder** reduces dimensionality and extracts essential transaction features.
- **Isolation Forest** detects anomalies based on learned representations.
- Efficient for **unsupervised learning**, detecting fraud without requiring labeled data.

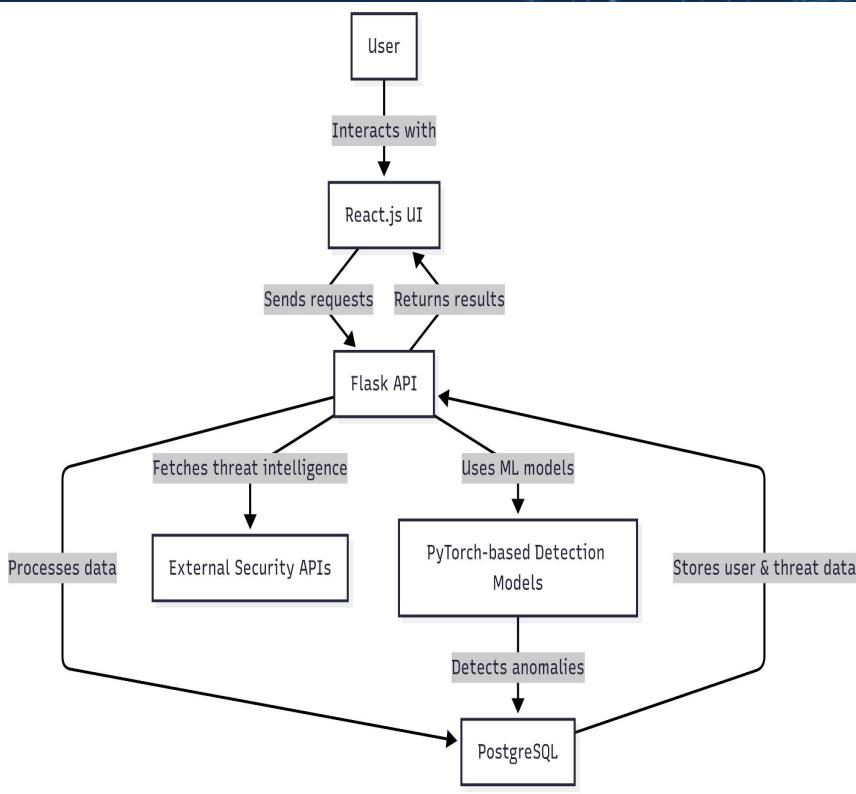
URL Classification:

Algorithm: CNN + LSTM (Convolutional Neural Network + Long Short-Term Memory)

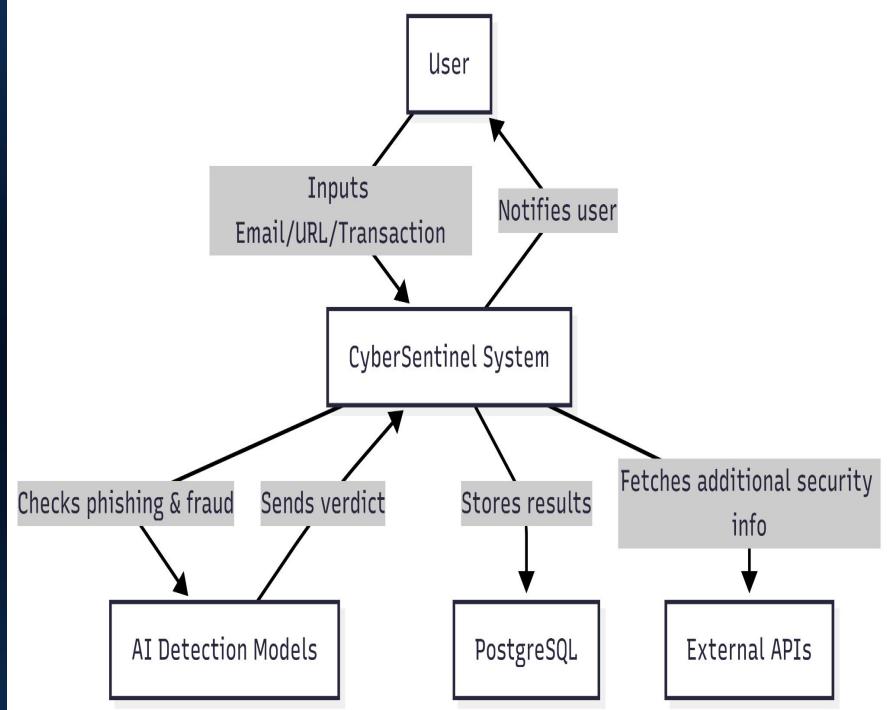
- **CNN extracts spatial features** from URL structure.
- **LSTM captures sequential patterns**, improving detection of phishing URLs.
- **Hybrid deep learning model** for better performance over traditional classifiers.

+++

Architecture Diagram

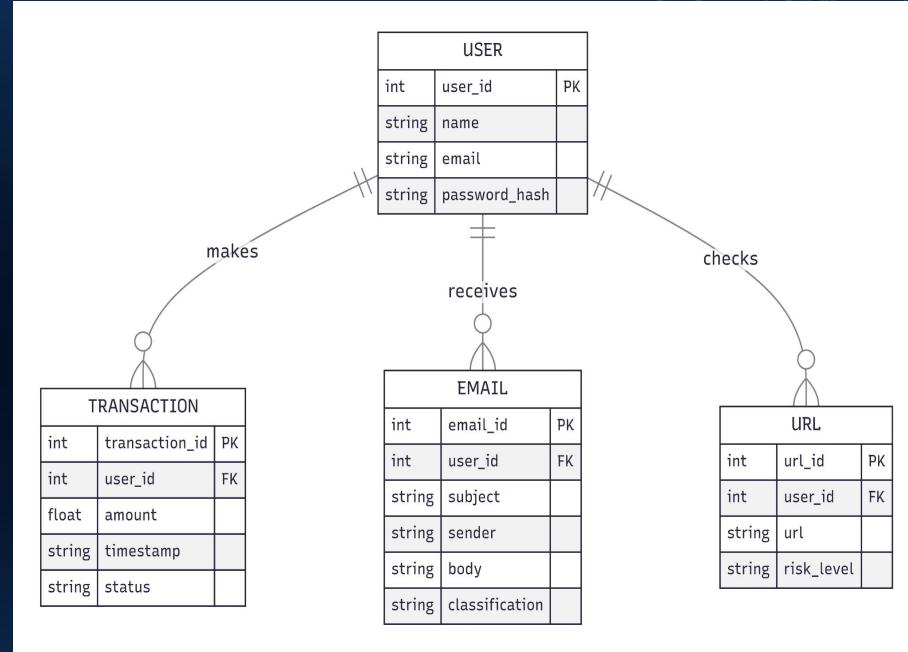


Context Diagram

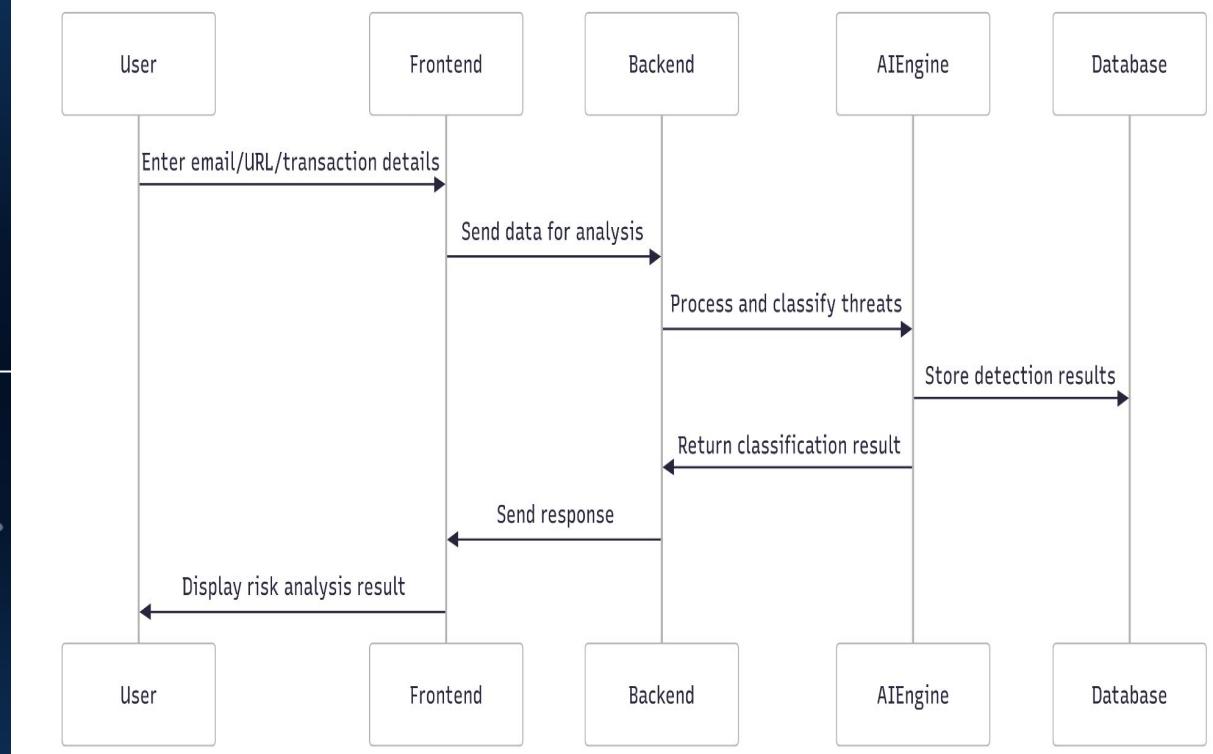


+++

ER Diagram

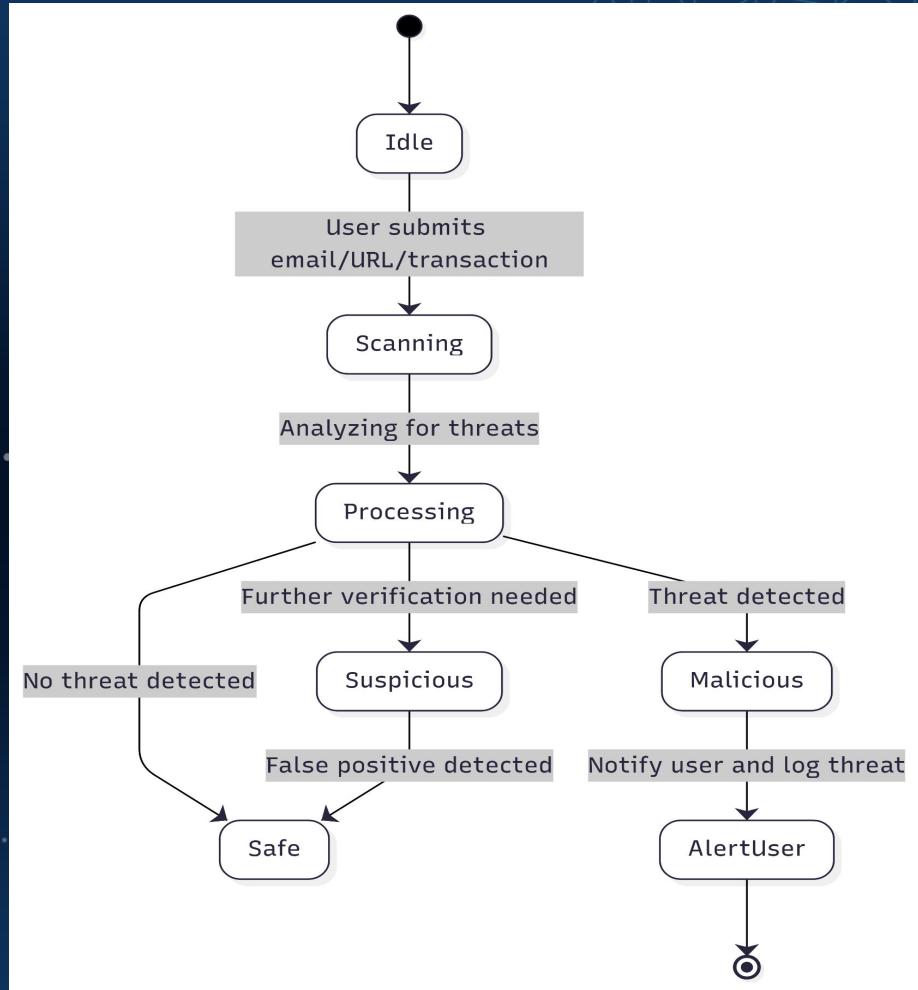


Sequence Diagram



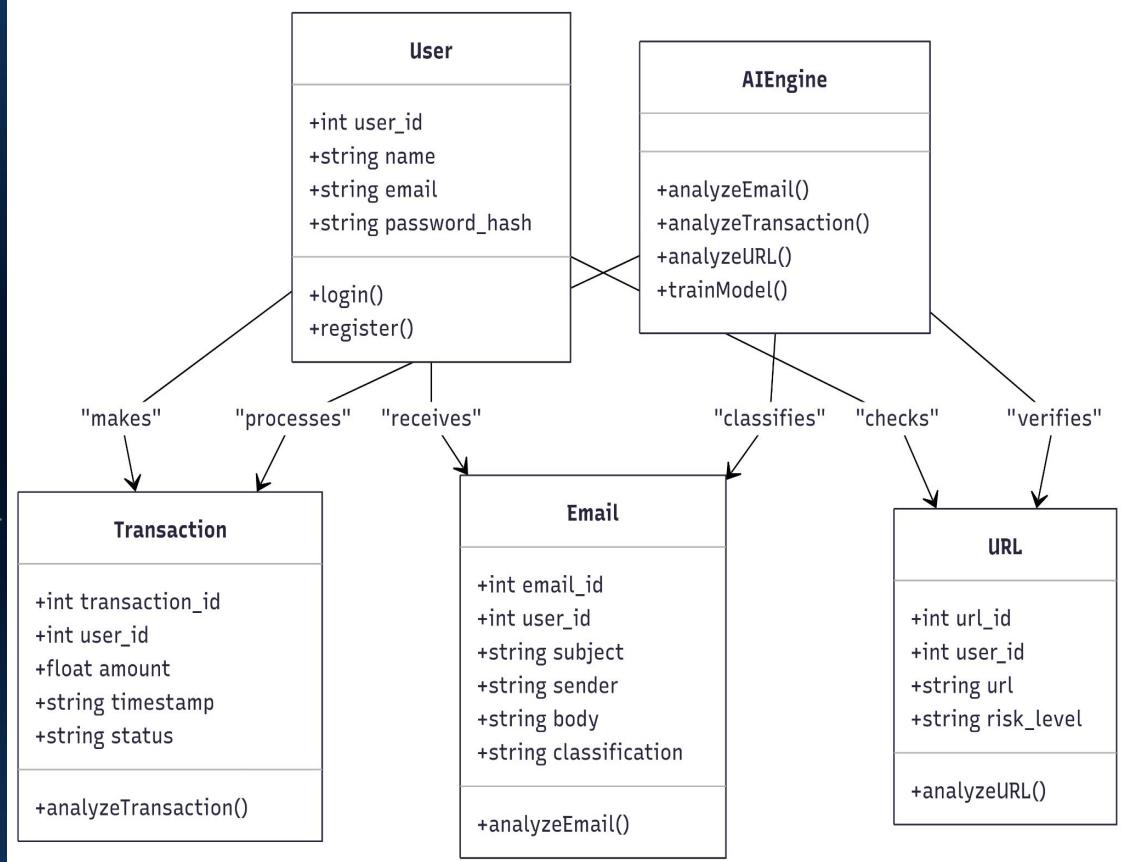
+++

State Diagram



+++

Class Diagram



Product Backlog - User Stories

ID	User Story	Acceptance Criteria	Sprint	Story Points
US_01	As someone monitoring threats, I want a dashboard to view phishing email history so that I can track past threats.	Dashboard displays list of phishing emails with filtering options.	Sprint 1	5
US_02	As an email recipient, I want to filter emails based on risk level so that I can quickly identify dangerous emails.	System allows filtering by safe, suspicious, and phishing categories.	Sprint 1	3
US_03	As a security admin, I want to view statistics on detected threats so that I can analyze system performance.	Dashboard provides statistics on phishing, fraud, and malicious URLs.	Sprint 1	8
US_04	As a platform administrator, I want to manage user roles and permissions so that I can control access levels.	System supports different access levels for users and admins.	Sprint 1	8
US_05	As an individual reviewing suspicious emails, I want to upload an email for phishing detection so that I can know if it's safe.	System classifies email as safe, suspicious, or phishing with an alert.	Sprint 2	8



Product Backlog - User Stories

ID	User Story	Acceptance Criteria	Sprint	Story Points
US_06	As a finance manager, I want to upload transaction data so that I can detect fraudulent activities.	System flags transaction as normal or suspicious with a confidence score.	Sprint 2	13
US_07	As someone browsing the web, I want to check if a URL is malicious so that I can avoid phishing sites.	System checks URL structure and domain reputation, classifying it as safe, suspicious, or malicious.	Sprint 2	5
US_08	As a cautious email reader, I want to verify if a sender email is trustworthy so that I can decide whether to engage with the sender.	System checks sender reputation and displays a trust score.	Sprint 2	8
US_09	As a system user, I want to receive real-time alerts for detected threats so that I can take immediate action.	User receives notifications via email or app for detected threats.	Sprint 3	8
US_10	As a user of the detection system, I want an option to report a false positive classification so that I can help improve detection accuracy.	Users can flag an incorrect detection for review.	Sprint 3	3



Product Backlog - Technical Stories

ID	Technical Story	Acceptance Criteria	Sprint	Story Points
TS_01	Create a dashboard for threat statistics so that admins can monitor system performance.	Dashboard displays data on detected threats.	Sprint 1	8
TS_02	Design a user role management system so that access levels can be controlled efficiently.	Admins can assign permissions to different user roles.	Sprint 1	8
TS_03	Implement OAuth authentication for secure user access so that users can log in securely.	User authentication is secure, and access tokens work correctly.	Sprint 1	5
TS_04	Set up AWS for cloud deployment so that the system can be scalable and accessible.	Backend deployed and accessible via API.	Sprint 1	5
TS_05	Integrate BERT model for phishing email detection so that emails can be classified accurately.	Model achieves at least 90% accuracy on test data.	Sprint 2	8



Product Backlog - Technical Stories

ID	Technical Story	Acceptance Criteria	Sprint	Story Points
TS_06	Implement Autoencoder + Isolation Forest for fraud detection so that anomalies in transactions can be detected.	Model correctly classifies anomalies in dataset.	Sprint 2	13
TS_07	Deploy CNN + LSTM model for URL detection so that phishing websites can be identified.	Model classifies URLs with at least 85% accuracy.	Sprint 2	8
TS_08	Implement email sender verification model so that sender reputation can be assessed.	System provides a sender trust score based on reputation.	Sprint 2	5
TS_09	Develop a notification system for real-time alerts so that users are informed of potential threats.	Users receive accurate notifications for detected threats.	Sprint 3	8
TS_10	Develop a feedback mechanism for false positive reports so that the system can improve over time.	Users can flag and submit incorrect classifications for review.	Sprint 3	3



Sprint 2 Backlog

ID	User Story / Task	Acceptance Criteria	Story Points
US_04	As an admin, I want to manage user roles and permissions so that I can control access levels.	System supports different access levels for users and admins.	8
TS_03	Implement OAuth authentication for secure user access so that users can log in securely.	User authentication is secure, and access tokens work correctly.	5
US_05	As an individual reviewing suspicious emails, I want to upload an email for phishing detection so that I can know if it's safe.	System classifies email as safe, suspicious, or phishing with an alert.	8
US_06	As a finance manager, I want to upload transaction data so that I can detect fraudulent activities.	System flags transaction as normal or suspicious with a confidence score.	13
US_07	As someone browsing the web, I want to check if a URL is malicious so that I can avoid phishing sites.	System checks URL structure and domain reputation, classifying it as safe, suspicious, or malicious.	5



Sprint 2 Backlog

ID	User Story / Task	Acceptance Criteria	Story Points
US_08	As a cautious email reader, I want to verify if a sender email is trustworthy so that I can decide whether to engage with the sender.	System checks sender reputation and displays a trust score.	8
TS_05	Integrate BERT model for phishing email detection so that emails can be classified accurately.	Model achieves at least 90% accuracy on test data.	8
TS_06	Implement Autoencoder + Isolation Forest for fraud detection so that anomalies in transactions can be detected.	Model correctly classifies anomalies in dataset.	13
TS_07	Deploy CNN + LSTM model for URL detection so that phishing websites can be identified.	Model classifies URLs with at least 85% accuracy.	8



Test Cases Sprint 2

Test Case ID	Story ID	Test Case	Expected Outcome	Actual Outcome	Pass/Fail
TC_01	US_04	Verify that admin can assign different roles to users (admin/user).	System successfully saves and applies roles, restricting access based on role type.	Roles not applied correctly; access not restricted.	Fail
TC_02	US_04	Attempt restricted action as a non-admin user.	Access is denied and appropriate error message is shown.	Action allowed for non-admin user.	Fail
TC_03	TS_03	Test OAuth login flow with valid credentials.	User logs in successfully and receives a valid access token.	Login unsuccessful; token not generated.	Fail
TC_04	TS_03	Test OAuth login with invalid credentials.	Login fails and user is prompted with an error message.	No proper error message shown; system crashes.	Fail
TC_05	US_05	Upload a phishing email sample for detection.	System classifies email as "phishing" and shows alert.	Email classified as phishing and alert displayed.	Pass



Test Cases Sprint 2

Test Case ID	Story ID	Test Case	Expected Outcome	Actual Outcome	Pass/Fail
TC_06	US_05	Upload a safe email sample.	System classifies email as "safe" without alerts.	Email correctly classified as safe.	Pass
TC_07	TS_05	Evaluate BERT model accuracy using test dataset.	Model reaches at least 90% classification accuracy.	Achieved 91.3% accuracy on test data.	Pass
TC_08	US_06	Upload a transaction with known fraud pattern.	System flags it as suspicious with high confidence score.	Flagged as suspicious with 92% confidence.	Pass
TC_09	US_06	Upload normal transaction data.	System classifies it as normal with a confidence score.	Classified as normal with 96% confidence.	Pass
TC_10	TS_06	Evaluate fraud detection model on test set.	Anomalies are correctly flagged in the dataset.	Anomalies detected with high accuracy.	Pass



Test Cases Sprint 2

Test Case ID	Story ID	Test Case	Expected Outcome	Actual Outcome	Pass/Fail
TC_11	US_07	Enter a known malicious URL.	System classifies it as "malicious".	URL detected as malicious.	Pass
TC_12	US_07	Enter a safe URL.	System classifies it as "safe".	URL classified as safe.	Pass
TC_13	TS_07	Run URL model on benchmark dataset.	Model classifies with minimum 85% accuracy.	Model achieved 87.5% accuracy.	Pass
TC_14	US_08	Submit sender email for reputation check.	System shows a trust score and message.	Sender trust score displayed correctly.	Pass



Sprint 2 Stories Completed

ID	User Story / Task	Story Points
US_05	As a user, I want to upload an email for phishing detection so that I can know if it's safe.	8
US_06	As a user, I want to upload transaction data so that I can detect fraudulent activities.	13
US_07	As a user, I want to check if a URL is malicious so that I can avoid phishing sites.	5
US_08	As a user, I want to verify if a sender email is trustworthy so that I can decide whether to engage with the sender.	8
TS_05	Integrate BERT model for phishing email detection so that emails can be classified accurately.	8
TS_06	Implement Autoencoder + Isolation Forest for fraud detection so that anomalies in transactions can be detected.	13
TS_07	Deploy CNN + LSTM model for URL detection so that phishing websites can be identified.	8

+++

Sprint 2 Stories Not Completed

ID	User Story / Task	Story Points
US_04	As an admin, I want to manage user roles and permissions so that I can control access levels.	8
TS_03	Implement OAuth authentication for secure user access so that users can log in securely.	5

Total Not Completed Story Points: 13



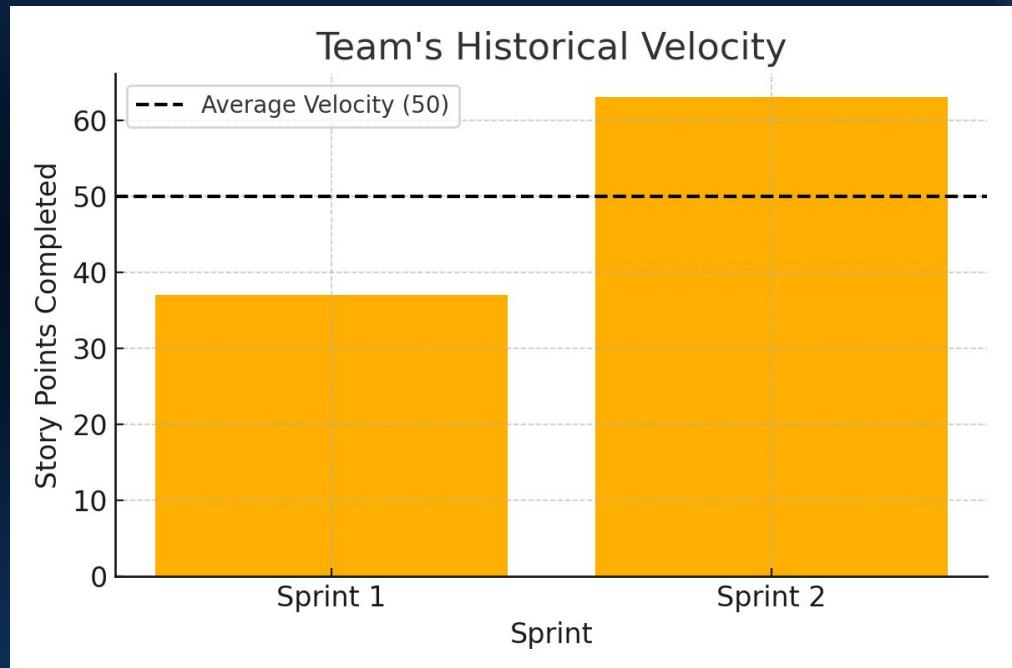
Team Velocity

Total Story Points Completed: 63

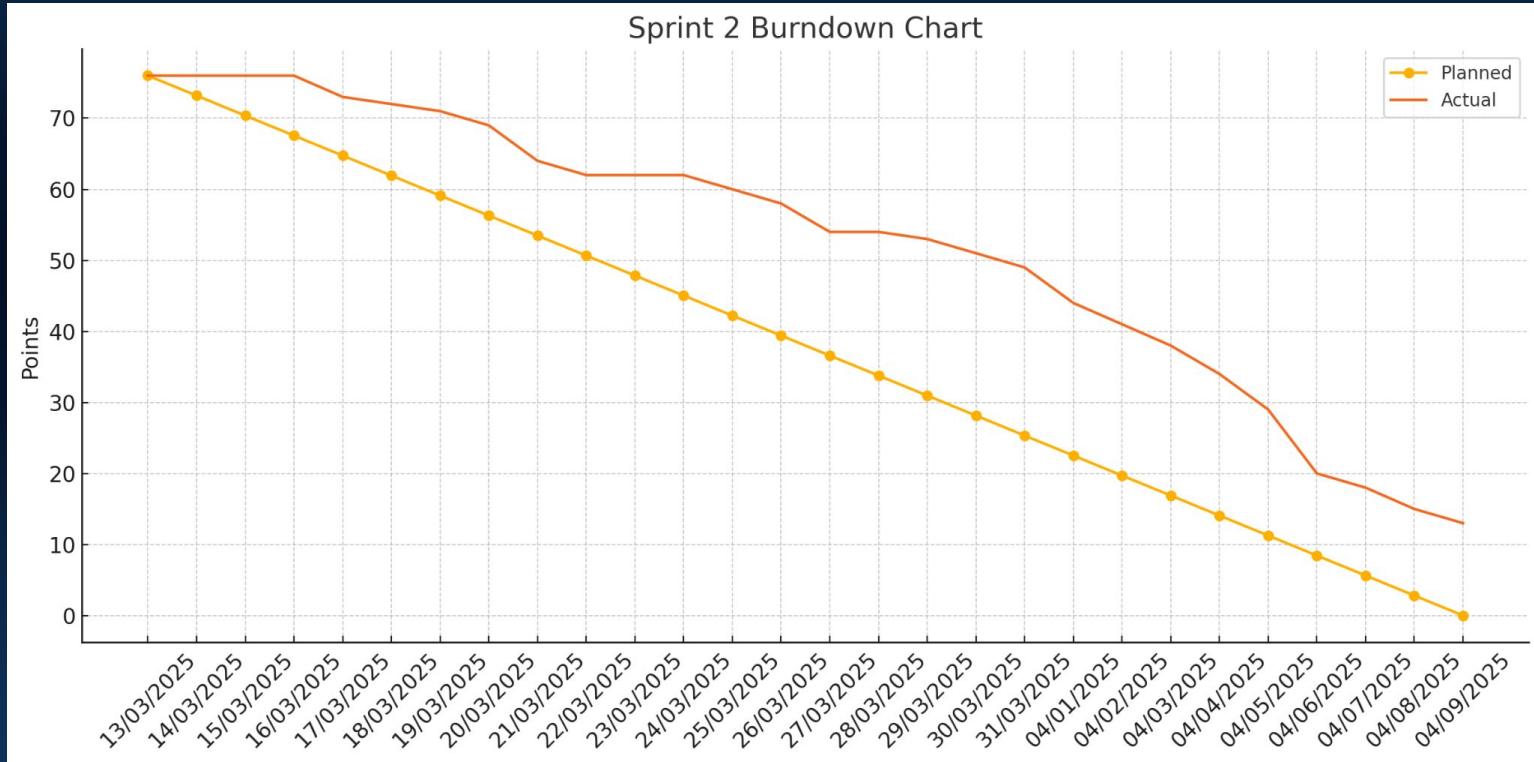


Team's Historical Velocity

- Sprint 1 Velocity: 37 story points
- Sprint 2 Velocity: 63 story points
- Average Velocity:
 $(37 + 63) / 2 = 50$ story points



Burn Down Chart



Completed/Committed Ratio



74%

Sprint 1



84.8%

Sprint 2



78.42%

Average Ratio



Retrospective

Sprint 3 Planning

ID	User Story	Acceptance Criteria	Story Points
US_09	As a system user, I want to receive real-time alerts for detected threats so that I can take immediate action.	User receives notifications via email or app for detected threats.	8
US_10	As a user of the detection system, I want an option to report a false positive classification so that I can help improve detection accuracy.	Users can flag an incorrect detection for review.	3
TS_09	Develop a notification system for real-time alerts so that users are informed of potential threats.	Users receive accurate notifications for detected threats.	8
TS_10	<ul style="list-style-type: none">Develop a feedback mechanism for false positive reports so that the system can improve over time.	Users can flag and submit incorrect classifications for review.	3
US_04 (Carry forward)	As a platform administrator, I want to manage user roles and permissions so that I can control access levels.	System supports different access levels for users and admins.	8
TS_03 (Carry forward)	Implement OAuth authentication for secure user access so that users can log in securely.	User authentication is secure, and access tokens work correctly.	5

Application Screenshots

CyberSentinel

3 A Alex Johnson Admin

Email Security Dashboard

Export Report Settings

Email Risk Summary

Overall security status

Phishing: 2
Suspicious: 2
Safe: 2

6

Malicious URLs

Detected in emails

Detected 7

Fraud Attempts

Blocked this week

Blocked 3

Weekly Summary

Threat trends

Total incidents 28

+12.5% from last week

Email Security Analysis

Review and monitor potentially dangerous emails

Risk Level All Risk Levels

Status All Statuses

Search Search by sender or subject...

Sender	Subject	Received	Risk Level	Status	Actions
noreply@amazon-security.com	Your Amazon account has been locked	Mar 10, 02:32 PM	Phishing	Flagged	...
updates@dropbox.com	Your shared document has been updated	Mar 10, 11:15 AM	Suspicious	Reviewing	...

Application Screenshots

Phishing: 2
Suspicious: 2
Safe: 2

6

Detected 7

Blocked 3

Total incidents 28
+12.5% from last week

Email Security Analysis

Review and monitor potentially dangerous emails

Risk Level: Suspicious

Status: All Statuses

Search: Search by sender or subject...

Sender	Subject	Received	Risk Level	Status	Actions
updates@dropbox.com	Your shared document has been updated	Mar 10, 11:15 AM	Suspicious	Reviewing	...
support@microsoft365.net	Your Office 365 password will expire soon	Mar 8, 02:52 PM	Suspicious	Reviewing	...

Showing 2 of 6 emails

Current role: Admin

Export Results

Application Screenshots

The screenshot shows a dark-themed web application interface. At the top, there is a navigation bar with two items: "Dashboard" and "Security Tools". Below the navigation bar, a section titled "Security Analysis Tools" is visible, with a sub-instruction "Analyze emails, transactions, and URLs for potential security threats". Underneath this, there are three buttons: "Email Analysis", "Transaction Fraud", and "URL Checker". A large, semi-transparent rectangular overlay covers the central part of the page. This overlay contains a section titled "Transaction Fraud Detection" with the sub-instruction "Upload transaction data to identify potentially fraudulent activities. Our system will analyze patterns and flag suspicious transactions." At the bottom left of this overlay, there is a button labeled "Analyze Transactions". In the bottom left corner of the main page area, there is a small circular icon containing the letter "N".

Dashboard

Security Tools

Security Analysis Tools

Analyze emails, transactions, and URLs for potential security threats

Email Analysis

Transaction Fraud

URL Checker

Transaction Fraud Detection

Upload transaction data to identify potentially fraudulent activities. Our system will analyze patterns and flag suspicious transactions.

Analyze Transactions

N

Application Screenshots

Email Risk Summary

Overall security status

- Phishing: 2
- Suspicious: 2
- Safe: 2

6

Dashboard Security

Security Analysis Tools

Analyze emails, transactions, and URLs for potential threats.

Email Analysis Transaction F...

URL Safety Checker

Check if a URL is potentially malicious.

Check URL Safety

URL Safety Checker

Analyze a URL to determine if it's potentially malicious or safe to visit.

Enter URL to check

Check

Enter a complete URL including http:// or https://

Safety Analysis 92% Confidence

⊕ <https://paypal1.com/verify/account>

Warning: Potentially Dangerous URL

Domain Information

- Domain Age: < 30 days
- Reputation: 15/100
- HTTPS: Valid
- Category: Uncategorized

Detected Issues

- Potential typosquatting attack (brand impersonation)

Recommendation

Do not visit this website. It has been identified as potentially harmful.

Check Another URL Close

Weekly Summary

Threat trends

Total incidents 28

+12.5% from last week

API Screenshots

POST http://localhost:3000/api/analyze-email

Params Authorization Headers (10) Body Scripts Tests Settings Cookies Beautify

Body raw binary GraphQL JSON

```
1 {  
2   "sender": "security@paypalI.com",  
3   "subject": "Urgent: Your PayPal account has been limited",  
4   "content": "Dear PayPal Customer,\n\nWe have detected unusual activity on your account and need to verify your information immediately. Your account access has been limited until this process is complete.\n\nPlease verify your information by clicking on the secure link below:\nhttps://paypal1-secure-verification.com/account/verify?id=12345\n\nFailure to verify your account within 24 hours will result in permanent suspension.\n\nThank you,\nPayPal Security Team"  
5 }  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15 }
```

Body Cookies Headers (9) Test Results

200 OK - 8.11 s - 1.3 KB - Save Response

Pretty Raw Preview Visualize JSON

```
1 {  
2   "riskLevel": "phishing",  
3   "confidence": 95,  
4   "indicators": [  
5     "Spoofed domains or typosquatting attempts",  
6     "Urgent language demanding immediate action",  
7     "Suspicious URL patterns",  
8     "Impersonation of trusted entities"  
9   ],  
10  "analysis": "The email exhibits several common phishing indicators. The sender's email address 'security@paypalI.com' uses a typosquatting technique by replacing the 'l' in 'PayPal' with a capital 'I'. The email uses urgent language to create a sense of panic, urging immediate action to avoid account suspension. The URL provided for verification is suspicious, as it does not belong to the official PayPal domain and uses a similar typosquatting technique. The email impersonates PayPal, a trusted entity, to deceive the recipient.",  
11  "suspiciousLinks": [  
12    "https://paypal1-secure-verification.com/account/verify?id=12345"  
13  ],  
14  "recommendedAction": "Do not click on any links or provide any personal information. Report the email to PayPal's phishing department and delete the email from your inbox."  
15 }
```

Github Wikipage Link

<https://github.com/htmw/2025S-Tech-Titans/wiki>

Application Demo

Thank You

