

The screenshot shows a web browser window with two tabs open, both titled "Cyber Threat Detection Framework". The active tab displays a login form with fields for "Username" and "Password", and a "Access Dashboard" button. Below the login form is a "Demo Access" section showing user credentials: "Administrator" (admin / admin123), "Security Analyst" (analyst / analyst123), and "Viewer" (viewer / viewer123). At the bottom is a "Security Features" section listing "Brute Force Protection", "Real-time Alerts", "Breach Detection", and "Anomaly Detection".

Cyber Threat Detection Framework X Cyber Threat Detection Framework X

http://localhost:8501

90% ⌂

Username

Enter your username

Password

Enter your password

Access Dashboard

Demo Access

Administrator admin / admin123

Security Analyst analyst / analyst123

Viewer viewer / viewer123

Brute Force Protection

Real-time Alerts

Breach Detection

Anomaly Detection



Cyber Threat Detection Framework X Cyber Threat Detection Framework X +

http://localhost:8501 90% Deploy

Configuration

Welcome, System Admin

DATA SOURCE

Upload Dataset (CSV)

Drag and drop file here
Limit 200MB per file • CSV

Browse files

sample_dataset.csv 2.8MB

ANALYSIS SETTINGS

Detection Mode

Anomaly Detection

Use PCA for Dimensionality Reduction

Air: Moderate Tomorrow

Cyber Threat Detection Framework

Advanced ML Ensembles + GNN for Cyber Security Analytics

System Admin Administrator Logout

Dataset loaded: 15000 rows, 31 columns

Encoding protocol_type categorical feature

Found 4 geographic columns: ['src_ip_encoded', 'dst_ip_encoded', 'src_country', 'dst_country']

Data preprocessing completed: 27 features, 3 classes

Data loaded successfully! Shape: (15000, 27)

Dataset Preview

Search

ENG IN 22:17 12-10-2025

This screenshot shows the Cyber Threat Detection Framework application running in a browser. The left sidebar contains sections for Configuration, DATA SOURCE (with a CSV file uploaded), and ANALYSIS SETTINGS (set to Anomaly Detection). The main area displays the application's branding and a message about using Advanced ML Ensembles + GNN for Cyber Security Analytics. It also shows a log of dataset processing steps: 'Dataset loaded: 15000 rows, 31 columns', 'Encoding protocol_type categorical feature', 'Found 4 geographic columns: ['src_ip_encoded', 'dst_ip_encoded', 'src_country', 'dst_country']', 'Data preprocessing completed: 27 features, 3 classes', and 'Data loaded successfully! Shape: (15000, 27)'. A 'Dataset Preview' section is partially visible at the bottom of the main area. The bottom of the screen shows a Windows taskbar with various icons and system status information.

Cyber Threat Detection Framework X Cyber Threat Detection Framework X +

http://localhost:8501 90% Deploy

Configuration

Welcome, System Admin

DATA SOURCE

Upload Dataset (CSV) Drag and drop file here Limit 200MB per file + CSV

Browse files

sample_dataset.csv 2.8MB

ANALYSIS SETTINGS

Detection Mode Anomaly Detection

Use PCA for Dimensionality Reduction

All models trained successfully!

PCA: Reduced from 27 to 25 components (96.56% variance explained)

Logistic Regression (PCA: 25 components): 93.233333% accuracy

SVM (PCA: 25 components): 93.866667% accuracy

Random Forest (PCA: 25 components): 86.933333% accuracy

K-Nearest Neighbors (PCA: 25 components): 84.766667% accuracy

XGBoost (PCA: 25 components): 98.300000% accuracy

Creating network graph for GNN analysis...

Graph created with 4668 nodes and 14646 edges

Training Graph Neural Network...

Air: Moderate Tomorrow

Search

ENG IN 22:17 12-10-2025

This screenshot shows the Cyber Threat Detection Framework application interface. On the left, there's a sidebar with sections for Configuration, DATA SOURCE (containing a CSV upload area with a sample dataset), and ANALYSIS SETTINGS (with a dropdown for Detection Mode set to Anomaly Detection and a checkbox for 'Use PCA for Dimensionality Reduction'). The main content area displays a log of model training progress. It includes success messages like 'All models trained successfully!' and various accuracy metrics for different models: Logistic Regression (93.233333%), SVM (93.866667%), Random Forest (86.933333%), K-Nearest Neighbors (84.766667%), and XGBoost (98.300000%). It also shows the process of creating a network graph for GNN analysis, stating 'Graph created with 4668 nodes and 14646 edges'. At the bottom, the taskbar shows system icons and the date/time (12-10-2025, 22:17). A notification bar at the top indicates 'Air: Moderate' and 'Tomorrow'.

Cyber Threat Detection Framework X Cyber Threat Detection Framework X +

http://localhost:8501 90% Deploy :

Configuration

Welcome, System Admin

DATA SOURCE

Upload Dataset (CSV) ?

Drag and drop file here
Limit 200MB per file • CSV

Browse files

sample_dataset.csv 2.8MB

ANALYSIS SETTINGS

Detection Mode

Anomaly Detection

Use PCA for Dimensionality Reduction

Air: Moderate Tomorrow

GNN nodes: 4668, Train samples: 12000, Test samples: 3000

Final dimensions - Train: (12000, 27), Test: (3000, 27)

Training XGBoost on hybrid features...

Hybrid GNN+XGBoost Accuracy: 98.800000%

Hybrid GNN+XGBoost: 98.800000% accuracy

Graph Analysis: Nodes: 4668, Edges: 14646

Model Performance Results

	Model	Accuracy (%)
4	XGBoost (PCA: 25 components)	98.800000
5	Hybrid GNN+XGBoost	98.800000
6	CNN (PCA: 25 components)	98.800000

Search ENG IN 22:17 12-10-2025

The screenshot shows a web-based application for cyber threat detection. On the left, there's a sidebar with sections for Configuration, DATA SOURCE (containing a CSV upload area with a sample dataset), and ANALYSIS SETTINGS (with options for Detection Mode set to Anomaly Detection and Use PCA for Dimensionality Reduction checked). The main content area displays various status messages and performance metrics. At the bottom right, there's a 'Model Performance Results' section with a table comparing three models based on accuracy. The table has columns for Model and Accuracy (%). The data rows are: Model 4 (XGBoost (PCA: 25 components)) with 98.800000%, Model 5 (Hybrid GNN+XGBoost) with 98.800000%, and Model 6 (CNN (PCA: 25 components)) with 98.800000%. The status bar at the bottom right shows system information like battery level, language (ENG), and date/time (12-10-2025).

Cyber Threat Detection Framework X Cyber Threat Detection Framework X + http://localhost:8501 90% Deploy

Configuration

Welcome, System Admin

DATA SOURCE

Upload Dataset (CSV) Drag and drop file here Limit 200MB per file • CSV

Browse files

sample_dataset.csv 2.8MB

ANALYSIS SETTINGS

Detection Mode Anomaly Detection

Use PCA for Dimensionality Reduction

Air: Moderate Tomorrow

Model Performance Results

Model	Accuracy (%)
XGBoost (PCA: 25 components)	99.800000
Hybrid GNN+XGBoost	99.800000
SVM (PCA: 25 components)	93.866667
Logistic Regression (PCA: 25 components)	93.233333
Random Forest (PCA: 25 components)	86.933333
K-Nearest Neighbors (PCA: 25 components)	84.766667

Model Accuracy Comparison

Model	Accuracy (%)
XGBoost	99.800000%
Hybrid GNN+XGBoost	99.800000%
SVM	93.866667%
Logistic Regression	93.233333%
Random Forest	86.933333%
K-Nearest Neighbors	84.766667%

22:17 12-10-2025

Cyber Threat Detection Framework X Cyber Threat Detection Framework X + http://localhost:8501 90% Deploy

Configuration

Welcome, System Admin

DATA SOURCE

Upload Dataset (CSV)

Drag and drop file here
Limit 200MB per file + CSV

Browse files

sample_dataset.csv 2.8MB

ANALYSIS SETTINGS

Detection Mode

Anomaly Detection

Use PCA for Dimensionality Reduction

Air: Moderate Tomorrow

Model Accuracy Comparison

Model Accuracy Comparison

Accuracy (%)

Models

Logistic Regression (PCA: 25 components) 93.233333%

SVM (PCA: 25 components) 93.866667%

Random Forest (PCA: 25 components) 86.933333%

K-Nearest Neighbors (PCA: 25 components) 84.799967%

XGBoost (PCA: 25 components) 98.800000%

Hybrid GNN/XGBoost 98.800000%

Precision

Recall

F1-Score

Detailed Metrics per Class

Select model from dropdown

Logistic Regression (PCA: 25 components)

ENG IN 22:18 12-10-2025

The screenshot displays the Cyber Threat Detection Framework interface. On the left, a sidebar titled 'Configuration' shows a welcome message for 'System Admin'. Under 'DATA SOURCE', there's a section for uploading a CSV dataset, with a file named 'sample_dataset.csv' (2.8MB) currently selected. Below this is the 'ANALYSIS SETTINGS' section, which includes a 'Detection Mode' dropdown set to 'Anomaly Detection' and a checked checkbox for 'Use PCA for Dimensionality Reduction'. A system status bar at the bottom indicates 'Air: Moderate' and 'Tomorrow'. The main content area features two charts. The top chart, titled 'Model Accuracy Comparison', is a bar chart showing accuracy percentages for six different models. The bottom chart, titled 'Detailed Metrics per Class', is a grouped bar chart showing precision, recall, and F1-score for the same six models. Both charts have their respective model names listed on the x-axis.

Cyber Threat Detection Framework X Cyber Threat Detection Framework X +

http://localhost:8501 90% Deploy

Configuration

Welcome, System Admin

DATA SOURCE

Upload Dataset (CSV)

Drag and drop file here
Limit 200MB per file + CSV

Browse files

sample_dataset.csv 2.8MB

ANALYSIS SETTINGS

Detection Mode

Anomaly Detection

Use PCA for Dimensionality Reduction

Air: Moderate Tomorrow

Precision Recall F1-Score

Detailed Metrics per Class

Select model from dropdown

Logistic Regression (PCA: 25 components)

All Confusion Matrices

Logistic Regression (PCA: 25 components) SVM (PCA: 25 components)

ENG IN 22:18 12-10-2025

The screenshot displays a web-based interface for a Cyber Threat Detection Framework. On the left, a sidebar titled 'Configuration' shows a 'DATA SOURCE' section where a CSV file named 'sample_dataset.csv' (2.8MB) has been uploaded. Below this, 'ANALYSIS SETTINGS' include 'Detection Mode' set to 'Anomaly Detection' and a checked 'Use PCA for Dimensionality Reduction' option. A notification at the bottom left indicates 'Air: Moderate Tomorrow'. The main content area features three bar charts under the heading 'Detailed Metrics per Class' for 'Logistic Regression (PCA: 25 components)'. The charts show Precision (~93%), Recall (~98%), and F1-Score (~93%) across three classes (0, 1, 2). At the bottom, there's a summary for 'All Confusion Matrices' comparing 'Logistic Regression (PCA: 25 components)' and 'SVM (PCA: 25 components)'. The browser status bar at the bottom right shows the date and time as '12-10-2025 22:18'.

Cyber Threat Detection Framework X Cyber Threat Detection Framework X +

http://localhost:8501 90% Deploy

Configuration

Welcome, System Admin

DATA SOURCE

Upload Dataset (CSV)

Drag and drop file here
Limit 200MB per file + CSV

Browse files

sample_dataset.csv 2.8MB

ANALYSIS SETTINGS

Detection Mode

Anomaly Detection

Use PCA for Dimensionality Reduction

Air: Moderate Tomorrow

All Confusion Matrices

Logistic Regression (PCA: 25 components) (Accuracy: 93.233333%)

Confusion Matrix - Logistic Regression (PCA: 25 components) (Accuracy: 93.233333%)

		Class 0	Class 1	Class 2
True Labels	Class 0	2343	456	456
	Class 1	456	1500	456
Class 2	456	456	1500	
	Count	2000	1500	1000

SVM (PCA: 25 components) (Accuracy: 93.866667%)

Confusion Matrix - SVM (PCA: 25 components) (Accuracy: 93.866667%)

		Class 0	Class 1	Class 2
True Labels	Class 0	2353	456	456
	Class 1	456	1500	456
Class 2	456	456	1500	
	Count	2000	1500	1000

Random Forest (PCA: 25 components)

K-Nearest Neighbors (PCA: 25 components)

Search ENG IN 22:18 12-10-2025

The screenshot displays a web-based application for cyber threat detection. On the left, a sidebar provides access to configuration, data source management (with a sample dataset uploaded), and analysis settings (set to Anomaly Detection). The main area is titled "All Confusion Matrices" and contains four separate confusion matrix plots. Each plot shows the count of true versus predicted labels for three classes (0, 1, 2) using Principal Component Analysis (PCA) with 25 components. The models shown are Logistic Regression, SVM, Random Forest, and K-Nearest Neighbors. All four models achieve an accuracy of approximately 93%. The confusion matrices are visualized as heatmaps where darker shades represent higher counts.

Cyber Threat Detection Framework X Cyber Threat Detection Framework X +

http://localhost:8501 90% Deploy

Configuration

Welcome, System Admin

DATA SOURCE

Upload Dataset (CSV)

Drag and drop file here
Limit 200MB per file + CSV

Browse files

sample_dataset.csv 2.8MB

ANALYSIS SETTINGS

Detection Mode

Anomaly Detection

Use PCA for Dimensionality Reduction

Air: Moderate Tomorrow

All Confusion Matrices

Logistic Regression (PCA: 25 components) (Accuracy: 93.233333%)

Confusion Matrix - Logistic Regression (PCA: 25 components) (Accuracy: 93.233333%)

		Class 0	Class 1	Class 2
True Labels	Class 0	2343	456	456
	Class 1	456	1500	456
Class 2	456	456	1500	
	Count	2000	1500	1000

SVM (PCA: 25 components) (Accuracy: 93.866667%)

Confusion Matrix - SVM (PCA: 25 components) (Accuracy: 93.866667%)

		Class 0	Class 1	Class 2
True Labels	Class 0	2353	456	456
	Class 1	456	1500	456
Class 2	456	456	1500	
	Count	2000	1500	1000

Random Forest (PCA: 25 components)

K-Nearest Neighbors (PCA: 25 components)

Search ENG IN 22:18 12-10-2025

Cyber Threat Detection Framework X Cyber Threat Detection Framework X + http://localhost:8501 90% Deploy

Welcome, System Admin

DATA SOURCE

Upload Dataset (CSV) Drag and drop file here Limit 200MB per file + CSV

Browse files sample_dataset.csv 2.8MB

ANALYSIS SETTINGS

Detection Mode Anomaly Detection

Use PCA for Dimensionality Reduction

Air: Moderate Tomorrow

Random Forest (PCA: 25 components)

Confusion Matrix - Random Forest (PCA: 25 components) (Accuracy: 86.933333%)

True Labels	Class 0	Class 1	Class 2
Class 0	2368	878	241
Class 1	878	1500	241
Class 2	241	241	1500

K-Nearest Neighbors (PCA: 25 components)

Confusion Matrix - K-Nearest Neighbors (PCA: 25 components) (Accuracy: 84.766667%)

True Labels	Class 0	Class 1	Class 2
Class 0	2341	412	369
Class 1	412	1500	369
Class 2	369	369	1500

XGBoost (PCA: 25 components)

Confusion Matrix - XGBoost (PCA: 25 components) (Accuracy: 98.800000%)

True Labels	Class 0	Class 1	Class 2
Class 0	2000	0	0
Class 1	0	2000	0
Class 2	0	0	2000

Hybrid GNN+XGBoost

Confusion Matrix - Hybrid GNN+XGBoost (Accuracy: 98.800000%)

True Labels	Class 0	Class 1	Class 2
Class 0	2000	0	0
Class 1	0	2000	0
Class 2	0	0	2000

Cyber Threat Detection Framework X Cyber Threat Detection Framework X +

http://localhost:8501 90% Deploy

Configuration

Welcome, System Admin

DATA SOURCE

Upload Dataset (CSV)

Drag and drop file here
Limit 200MB per file • CSV

Browse files

sample_dataset.csv 2.8MB

ANALYSIS SETTINGS

Detection Mode

Anomaly Detection

Use PCA for Dimensionality Reduction

Air: Moderate Tomorrow

XGBoost (PCA: 25 components)

Confusion Matrix - XGBoost (PCA: 25 components)
(Accuracy: 98.80000%)

True Labels	Class 0	Class 1	Class 2
Class 0	2355	808	0
Class 1	0	2355	808
Class 2	0	0	2355

Hybrid GNN+XGBoost

Confusion Matrix - Hybrid GNN+XGBoost
(Accuracy: 98.80000%)

True Labels	Class 0	Class 1	Class 2
Class 0	2355	808	0
Class 1	0	2355	808
Class 2	0	0	2355

Feature Importance Analysis

Hybrid GNN+XGBoost - Feature Importance

ENG IN 22:18 12-10-2025

Cyber Threat Detection Framework X Cyber Threat Detection Framework X +

http://localhost:8501 90% Deploy

Configuration

Welcome, System Admin

DATA SOURCE

Upload Dataset (CSV) Drag and drop file here Limit 200MB per file + CSV

Browse files

sample_dataset.csv 2.8MB

ANALYSIS SETTINGS

Detection Mode Anomaly Detection

Use PCA for Dimensionality Reduction

Air: Moderate Tomorrow

Search

Feature Importance Analysis

Hybrid GNN+XGBoost - Feature Importance

Top 15 Most Important Features

Feature	Importance
dst_host_serror_rate	0.005
dst_host_count	0.005
dst_host_same_src_port_rate	0.005
num_access_files	0.005
serror_rate	0.005
count	0.005
duration	0.005
hot	0.006
proto_tcp	0.006
srv_serror_rate	0.006
num_compromised	0.006
logged_in	0.007
root_shell	0.108

ENG IN 22:19 12-10-2025

Cyber Threat Detection Framework X Cyber Threat Detection Framework X +

http://localhost:8501 90% Deploy :

Configuration Welcome, System Admin

DATA SOURCE

Upload Dataset (CSV) Drag and drop file here Limit 200MB per file + CSV

Browse files

sample_dataset.csv 2.8MB

ANALYSIS SETTINGS

Detection Mode Anomaly Detection

Use PCA for Dimensionality Reduction

Air: Moderate Tomorrow

Advanced Geographical Threat Analysis

World Map Threat Distribution

Threat Origins by Source Country

src_bytes 0.313

num_failed_logins 0.474

Feature Importance

This screenshot shows the Cyber Threat Detection Framework application interface. On the left, there's a sidebar with 'Configuration' and 'Welcome, System Admin'. Below it is a 'DATA SOURCE' section with a CSV upload area containing 'sample_dataset.csv' (2.8MB). Under 'ANALYSIS SETTINGS', 'Anomaly Detection' is selected. A checkbox for 'Use PCA for Dimensionality Reduction' is checked. At the bottom left, there's a notification for 'Air: Moderate Tomorrow'. The main content area features a 'Feature Importance' chart with two bars: 'src_bytes' at 0.313 and 'num_failed_logins' at 0.474. Below this is a section titled 'Advanced Geographical Threat Analysis' with a 'World Map Threat Distribution' chart. The map shows threat origins by source country, with a color scale from white to dark purple representing 'threat_count' from 2000 to 4000. The USA is shown in dark purple.

Cyber Threat Detection Framework X Cyber Threat Detection Framework X + http://localhost:8501 90% Deploy

Configuration

Welcome, System Admin

DATA SOURCE

Upload Dataset (CSV) Drag and drop file here Limit 200MB per file + CSV

Browse files

sample_dataset.csv 2.8MB

ANALYSIS SETTINGS

Detection Mode Anomaly Detection

Use PCA for Dimensionality Reduction

Air: Moderate Tomorrow

Threat Targets by Destination Country

Detailed Country-Threat Analysis

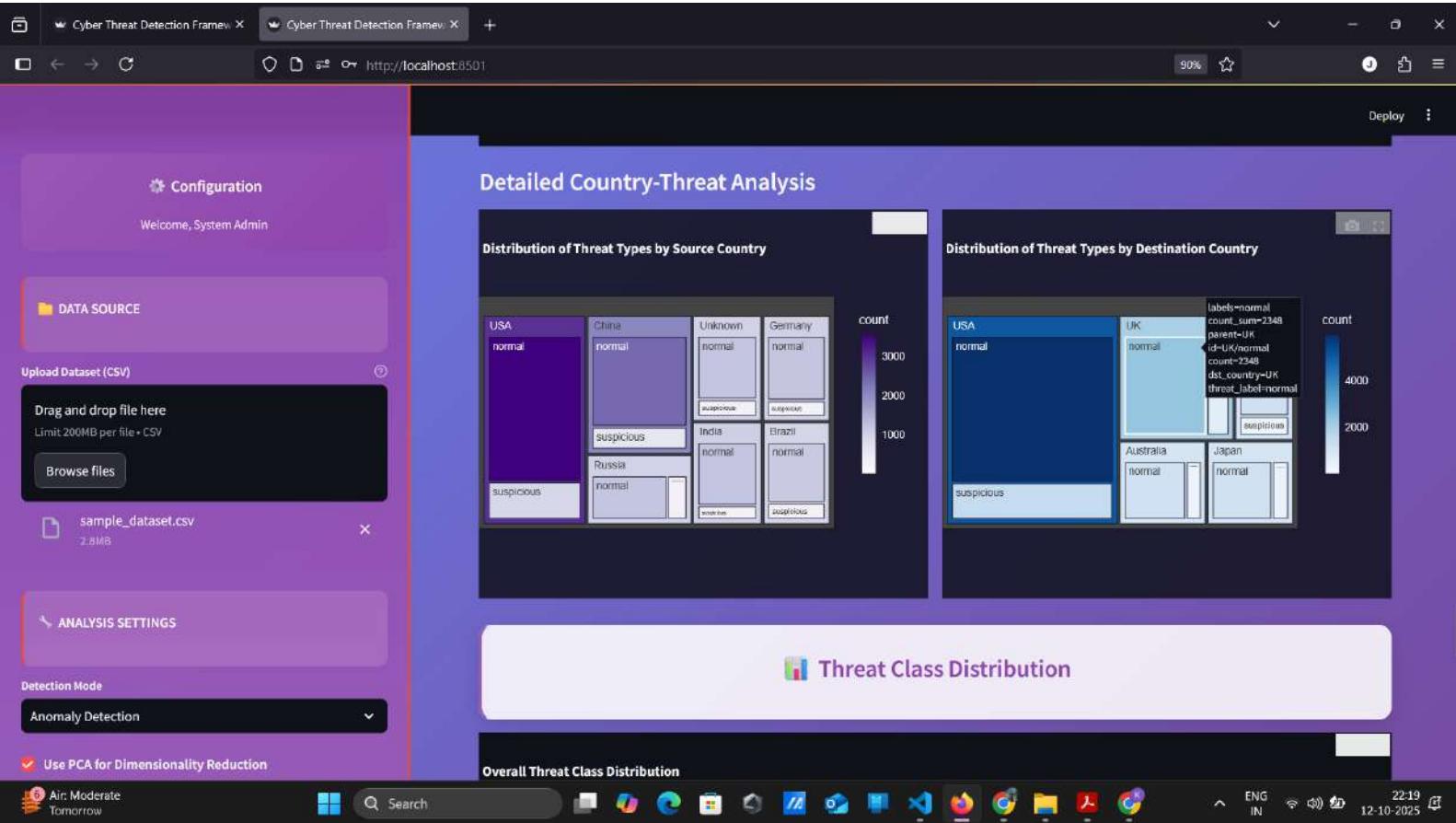
Distribution of Threat Types by Source Country

Country	Status	Count
USA	normal	3000
China	normal	2500
Unknown	normal	2000
Germany	normal	2000

Distribution of Threat Types by Destination Country

Country	Status	Count
USA	normal	4000
UK	normal	3500
Canada	normal	3000

This screenshot shows the Cyber Threat Detection Framework application interface. On the left, there's a sidebar with 'Configuration' and 'DATA SOURCE' sections. The 'DATA SOURCE' section includes a CSV upload area with a 'sample_dataset.csv' file listed. Below it are 'ANALYSIS SETTINGS' with 'Anomaly Detection' selected and a PCA dimensionality reduction checkbox. At the bottom left, there's a system status bar with 'Air: Moderate Tomorrow'. The main content area has a dark header 'Threat Targets by Destination Country' with a world map heatmap where North America is dark purple (highest threat count). Below it is a section titled 'Detailed Country-Threat Analysis' with two bar charts: 'Distribution of Threat Types by Source Country' (USA ~3000, China ~2500, Unknown ~2000, Germany ~2000) and 'Distribution of Threat Types by Destination Country' (USA ~4000, UK ~3500, Canada ~3000). The bottom right shows a Windows taskbar with various icons and the date/time '12-10-2025 22:19'.





 Network Flow Analysis

Cyber Threat Detection Framework X Cyber Threat Detection Framework X +

http://localhost:8501 90% Deploy

Configuration

Welcome, System Admin

DATA SOURCE

Upload Dataset (CSV) Drag and drop file here Limit 200MB per file + CSV

Browse files

sample_dataset.csv 2.8MB

ANALYSIS SETTINGS

Detection Mode Anomaly Detection

Use PCA for Dimensionality Reduction

28°C Mostly clear Search

Network Flow Analysis

Top 10 Threat Flows (Source → Destination)

SRC_Country	Count
Brazil	~600
Germany	~600
Unknown	~600
India	~600
Russia	~600
China	~3500
USA	~3200

Export Results

ENG IN 22:19 12-10-2025

Cyber Threat Detection Framework X Cyber Threat Detection Framework X + http://localhost:8501 90% Deploy

Anomaly Detection

Use PCA for Dimensionality Reduction

Analyze Threats

BREACH PROTECTION

Detection Sensitivity:

Minimum Confidence:

Auto-Quarantine Suspicious Nodes

Block Malicious IPs

Real-time Security Alerts

Backup Critical Data

Detect & Protect

System Admin Administrator Logout

Cyber Threat Detection Framework

Advanced ML Ensembles + GNN for Cyber Security Analytics

Analyzing network data for breach patterns...

Breach protection analysis completed!

Breach Detection Overview

Potential Breaches	High Risk Incidents	Protected Assets	Prevention Rate
9595	8193	1	0.0%

Detected Breach Types

28°C Mostly clear Search ENG IN 22:20 12-10-2025

The screenshot shows a web-based interface for a Cyber Threat Detection Framework. On the left, a sidebar titled 'Anomaly Detection' contains settings for 'Use PCA for Dimensionality Reduction', a button to 'Analyze Threats', and a 'BREACH PROTECTION' section with sliders for 'Detection Sensitivity' and 'Minimum Confidence'. It also lists several security features with checkboxes: 'Auto-Quarantine Suspicious Nodes', 'Block Malicious IPs', 'Real-time Security Alerts', and 'Backup Critical Data'. Below these is a 'Detect & Protect' button. The main content area has a purple header with the title 'Cyber Threat Detection Framework' and subtitle 'Advanced ML Ensembles + GNN for Cyber Security Analytics'. It displays two status messages: 'Analyzing network data for breach patterns...' and 'Breach protection analysis completed!'. A large callout box titled 'Breach Detection Overview' provides a summary of detected threats: 9595 potential breaches, 8193 high-risk incidents, 1 protected asset, and a 0.0% prevention rate. At the bottom, there's a 'Detected Breach Types' section which is currently empty. The bottom of the screen shows a Windows taskbar with various icons and system status information like weather and date.

Cyber Threat Detection Framework X Cyber Threat Detection Framework X + http://localhost:8501 90% Deploy

Anomaly Detection

Use PCA for Dimensionality Reduction

Analyze Threats

BREACH PROTECTION

Detection Sensitivity:

Minimum Confidence:

Auto-Quarantine Suspicious Nodes

Block Malicious IPs

Real-time Security Alerts

Backup Critical Data

Detect & Protect

Detected Breach Types

Breach Type	Count
data_exfiltration	~500
statistical_anomaly	~3800
suspicious_activity	~4800
privilege_escalation	~100

Detailed Breach Analysis

Type	Description	Confidence	Risk Score	Severity
0 Data Exfiltration	Large data transfer to USA	0.99	9.9	High
1 Statistical Anomaly	Statistical anomaly in duration	0.94	9.4	High

28°C Mostly clear Search ENG IN 22:20 12-10-2025

Cyber Threat Detection Framework X Cyber Threat Detection Framework X + http://localhost:8501 90% Deploy

Anomaly Detection

Use PCA for Dimensionality Reduction

Analyze Threats

BREACH PROTECTION

Detection Sensitivity:

Minimum Confidence:

Auto-Quarantine Suspicious Nodes

Block Malicious IPs

Real-time Security Alerts

Backup Critical Data

Detailed Breach Analysis

	Type	Description	Confidence	Risk Score	Severity
0	Data Exfiltration	Large data transfer to USA	0.99	9.9	High
1	Statistical Anomaly	Statistical anomaly in duration	0.94	9.4	High
2	Statistical Anomaly	Statistical anomaly in duration	0.94	9.4	High
3	Statistical Anomaly	Statistical anomaly in duration	0.94	9.4	High
4	Statistical Anomaly	Statistical anomaly in duration	0.94	9.4	High
5	Statistical Anomaly	Statistical anomaly in duration	0.94	9.4	High
6	Statistical Anomaly	Statistical anomaly in duration	0.94	9.4	High
7	Statistical Anomaly	Statistical anomaly in duration	0.94	9.4	High
8	Statistical Anomaly	Statistical anomaly in duration	0.94	9.4	High
9	Statistical Anomaly	Statistical anomaly in duration	0.94	9.4	High

Protection Actions Taken

Action	Status	Impact

28°C Mostly clear Search Action Center 12-10-2025 22:20 ENG IN

Cyber Threat Detection Framework X Cyber Threat Detection Framework X + http://localhost:8501 90% Deploy

Anomaly Detection

Use PCA for Dimensionality Reduction

Analyze Threats

BREACH PROTECTION

Detection Sensitivity:

Minimum Confidence:

Auto-Quarantine Suspicious Nodes

Block Malicious IPs

Real-time Security Alerts

Backup Critical Data

Detect & Protect

Protection Actions Taken

Action	Status	Impact
0 Auto Quarantine	✗ Not Applied	Low
1 Block Malicious IPs	✓ Implemented	High
2 Security Alerts	✓ Implemented	High

Security Alerts

MEDIUM: Blocked malicious IP: Unknown

CRITICAL: data_exfiltration: Large data transfer to USA (Confidence: 0.99)

CRITICAL: statistical_anomaly: Statistical anomaly in duration (Confidence: 0.94)

CRITICAL: statistical_anomaly: Statistical anomaly in duration (Confidence: 0.94)

28°C Mostly clear Search ENG IN 22:20 12-10-2025

Cyber Threat Detection Framework X Cyber Threat Detection Framework X + http://localhost:8501 90% Deploy

Anomaly Detection

Use PCA for Dimensionality Reduction

Analyze Threats

BREACH PROTECTION

Detection Sensitivity: 10

Minimum Confidence: 0.10

Auto-Quarantine Suspicious Nodes

Block Malicious IPs

Real-time Security Alerts

Backup Critical Data

Detect & Protect

Security Alerts Implemented

Security Alerts

MEDIUM: Blocked malicious IP: Unknown

CRITICAL: data_exfiltration: Large data transfer to USA (Confidence: 0.99)

CRITICAL: statistical_anomaly: Statistical anomaly in duration (Confidence: 0.94)

Download Protection Report

28°C Mostly clear Search ENG IN 22:20 12-10-2025