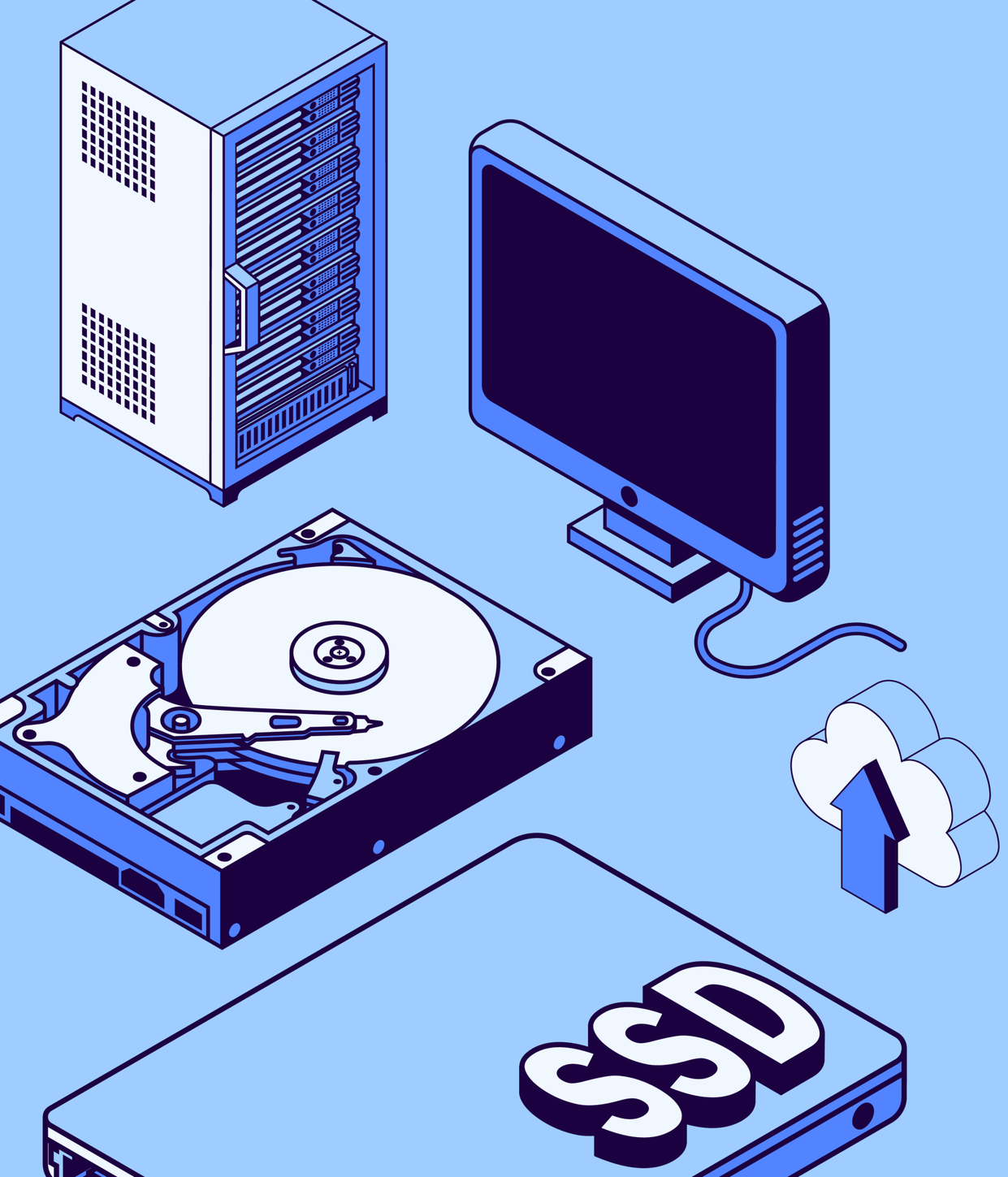
SecureLens: Intelligent Insider Threat Detection

Team Name : Quatrix

Bodhana A (23MA1030)
Hemila Saravanan (23MIA1048)
Divya P (23MIA1099)
Lokireddy Madhavi (23MIA1135)



Introduction

- Insider threats are one of the most critical cybersecurity risks, as they originate from trusted users within an organization.
- Traditional anomaly detection methods often fail to capture temporal patterns, lack privacy preservation, and operate as black-box models with little interpretability.
- Our project proposes an AI-powered Insider Threat Detection System that integrates:
- AI-driven anomaly detection **(Isolation Forest + Autoencoder).**
- **GRU Autoencoder** for detecting anomalies in sequential user activity.
- **Federated Learning** to ensure privacy-preserving, distributed model training.
- This approach enhances accuracy, privacy and trust in insider threat detection making it both practical and innovative.

Problem Statement

Insider threats are difficult to detect as they originate from trusted employees or contractors with legitimate access to systems. The goal is to develop an AI-powered system that continuously monitors user activities, including file access, login times, and application usage, to detect abnormal patterns indicating malicious intent or policy violations, and to alert security teams in real time.

Dataset

Sources Used:

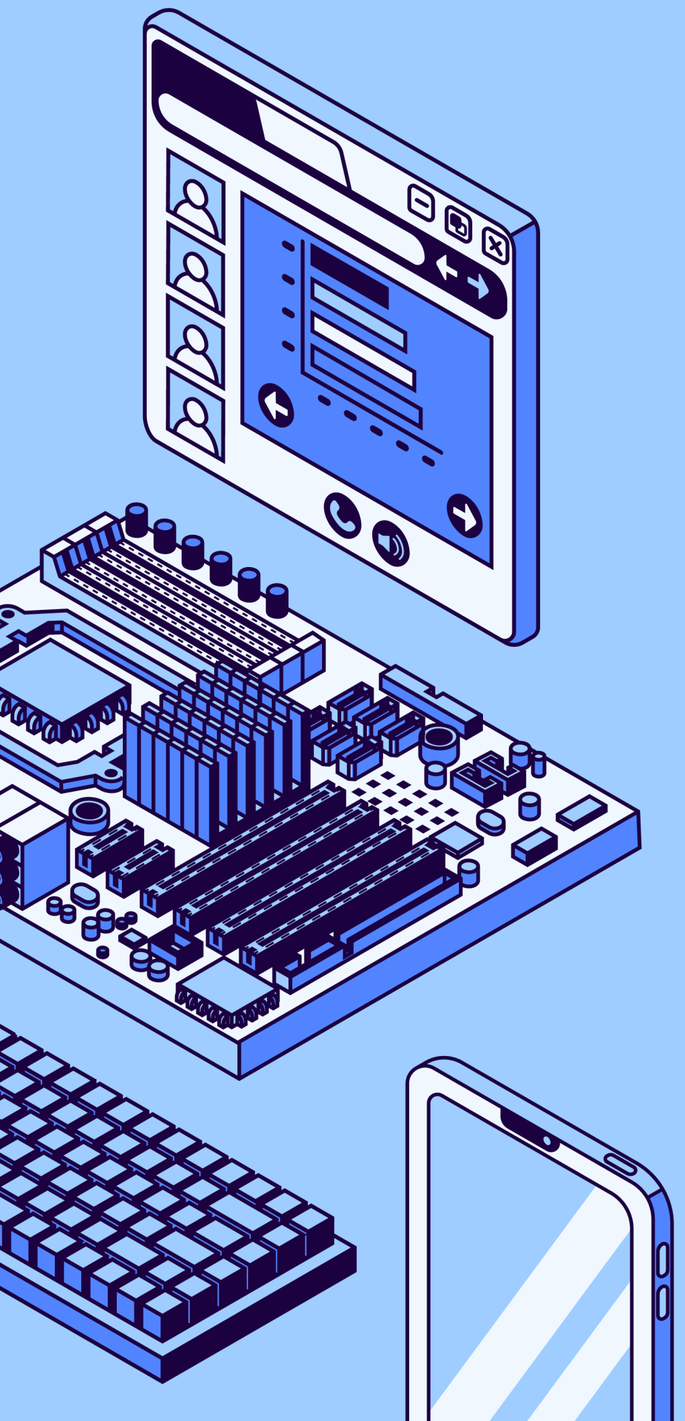
- File Access Logs → suspicious or excessive file interactions.
- Login Records → unusual login times or multiple failed attempts.
- USB Usage → unauthorized device connections.

Features Extracted:

- Login hours, file access frequency, USB events.

Merged dataset built for anomaly detection.

Flowchart



Input datasets (File, Login, USB).

Feature extraction & merging.

ML Models Isolation Forest + Autoencoder

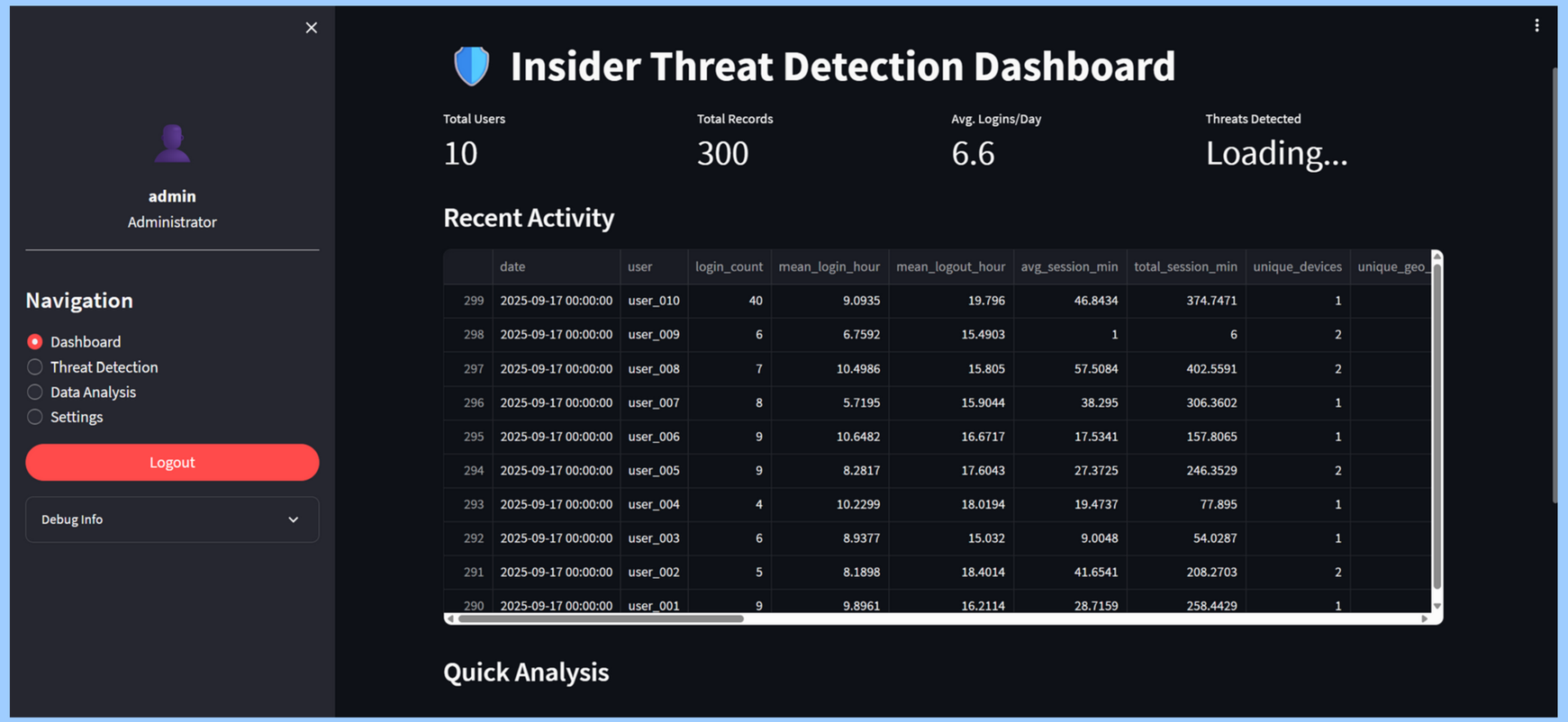
Federated Learning + Deep Learning

Anomaly scores assigned Risk levels (High/Medium/Low)

Dashboard output Threat ID, Source Dataset, Risk Score.

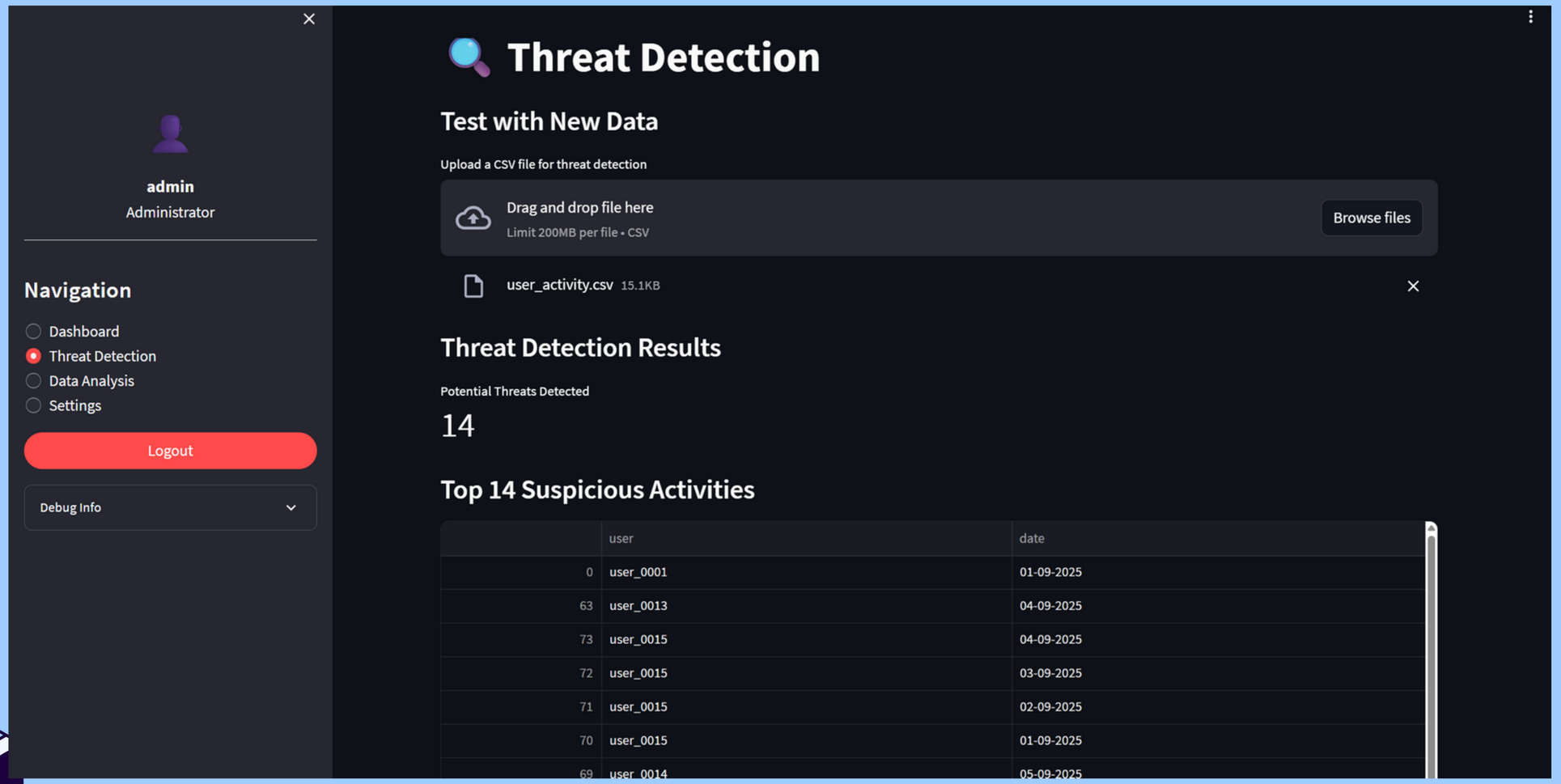
Dashboard Design

Dashboard Design

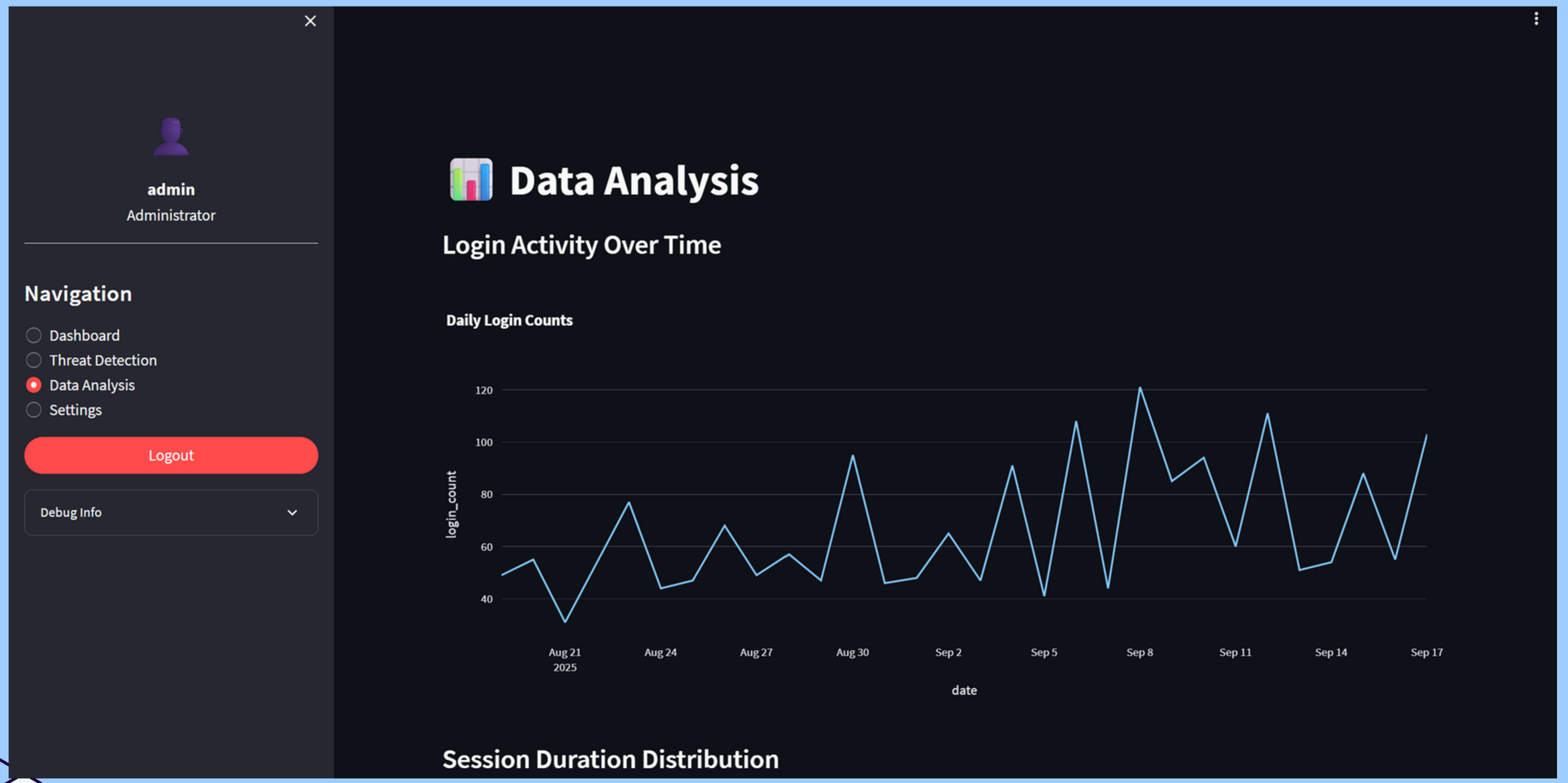


	date	user	login_count	mean_login_hour	mean_logout_hour	avg_session_min	total_session_min	unique_devices	unique_geo_
299	2025-09-17 00:00:00	user_010	40	9.0935	19.796	46.8434	374.7471	1	
298	2025-09-17 00:00:00	user_009	6	6.7592	15.4903	1	6	2	
297	2025-09-17 00:00:00	user_008	7	10.4986	15.805	57.5084	402.5591	2	
296	2025-09-17 00:00:00	user_007	8	5.7195	15.9044	38.295	306.3602	1	
295	2025-09-17 00:00:00	user_006	9	10.6482	16.6717	17.5341	157.8065	1	
294	2025-09-17 00:00:00	user_005	9	8.2817	17.6043	27.3725	246.3529	2	
293	2025-09-17 00:00:00	user_004	4	10.2299	18.0194	19.4737	77.895	1	
292	2025-09-17 00:00:00	user_003	6	8.9377	15.032	9.0048	54.0287	1	
291	2025-09-17 00:00:00	user_002	5	8.1898	18.4014	41.6541	208.2703	2	
290	2025-09-17 00:00:00	user_001	9	9.8961	16.2114	28.7159	258.4429	1	

Dashboard Design

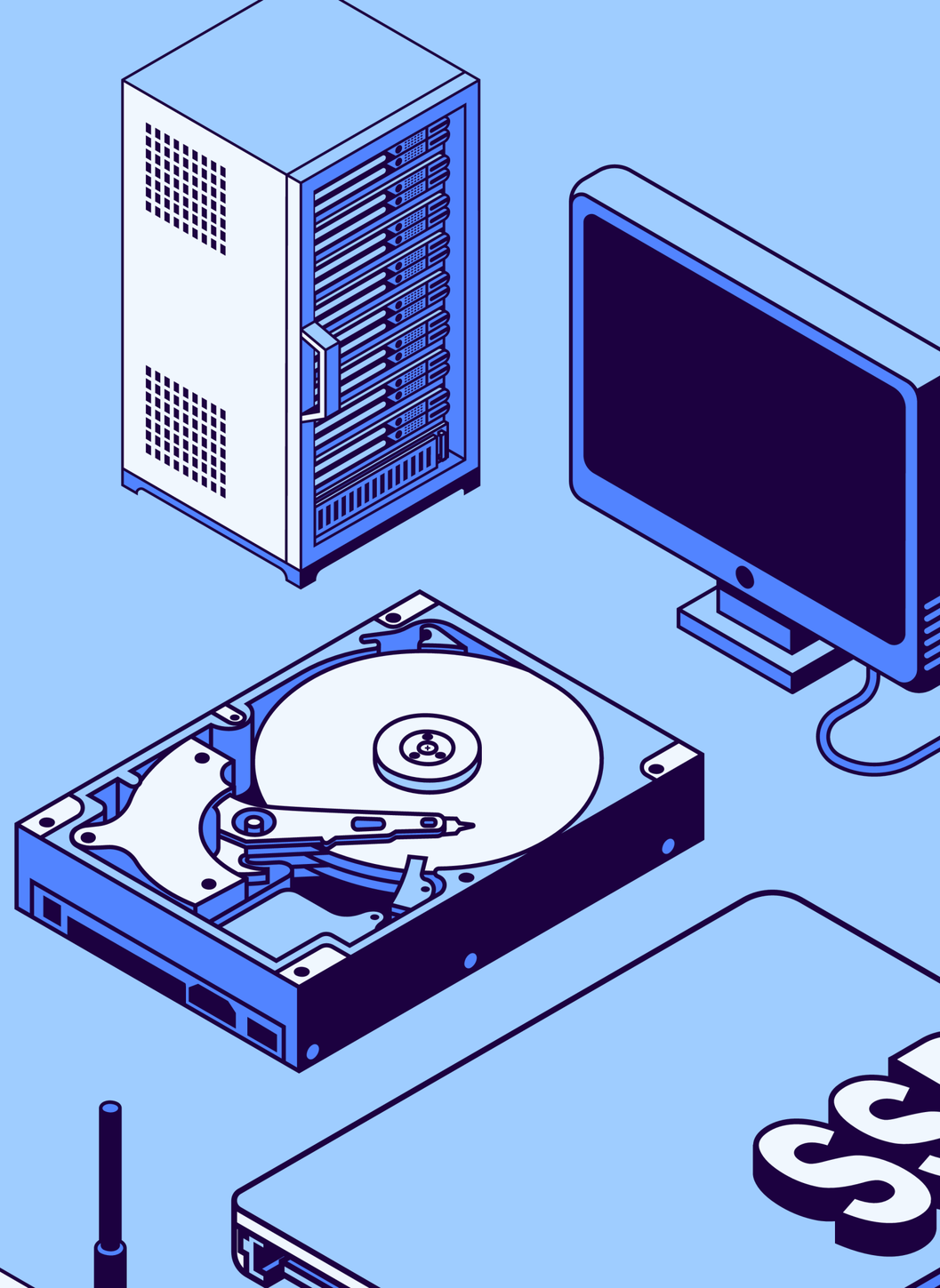


Dashboard Design



Outcomes

- AI-driven anomaly detection from merged activity datasets.
- Risk scoring for prioritized response.
- Secure, authenticated dashboard - prevents unauthorized viewing.
- Quick insights for SOC teams: who to investigate first.
- Demo-friendly, practical solution implementable in enterprises.



Novelty

- Uses dual ML approach (Isolation Forest + Autoencoder) for robust anomaly detection.
- **Federated learning + Deep Learning (GRU Autoencoder)**
- Secure dashboard with authentication - ensures only trusted authority sees sensitive alerts.

Thank You