AI JUGAAD SQUAD

Protecting the Digital World

AI for Digital Security

-

About Us

INTRODUCING AI JUGAAD SQUAD's TEAM MEMBERS

TEAM LEADER

- RAKSHIT RAJ

TEAM MEMBERS

- ARYAN AMIT ARYA
- SHRENIKA RAJPOOT
- DILISHA

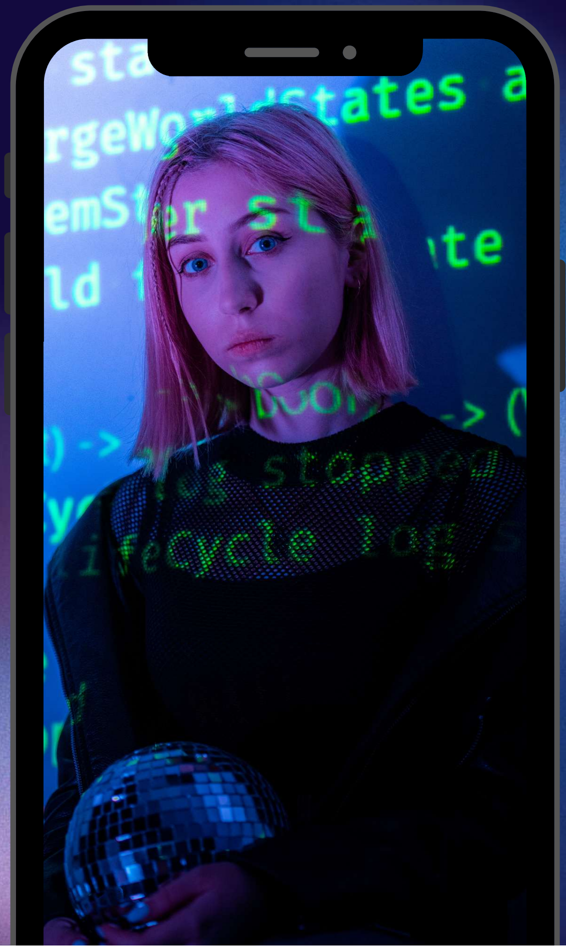
AI JUGAAD SQUAD

~ 2025 BATCH

Problem Statement

👉 Modern technological and cyber threats, such as advanced cyber-attacks, autonomous weapon systems, and manipulated information streams, have become so fast, numerous, and complex that traditional human abilities for detection, analysis, and response are insufficient.

👉 Human teams are now routinely outpaced by automated attacks, persistent threat actors, and rapidly evolving malicious tactics, leading to heightened security, economic, and safety risks.



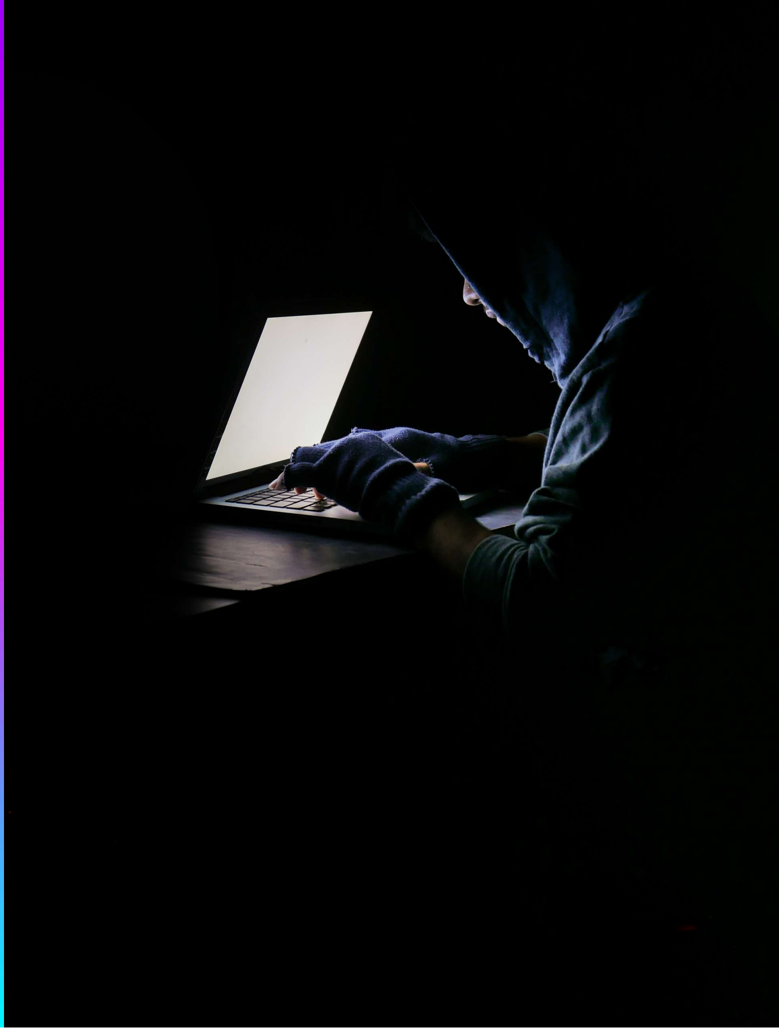
Relevance

- 📊 **Escalating Risks:** Critical infrastructure, personal data, and national security now face continuous and automated threats, making manual monitoring and intervention obsolete and increasing systemic vulnerabilities.

- 🤖 **AI and Automation:** The use of AI in both attacks and defense has created an arms race, with attackers automating their methods to penetrate defenses faster than human teams can respond.

- 📰 **Societal Impact:** These threats can disrupt economies, influence political stability, and even pose existential risks through technologies that exceed regulatory and ethical controls.

- 📝 **Need for New Solutions:** This environment necessitates advancing automated, intelligent, and adaptive security systems that can keep pace with evolving threats and minimize the overwhelming burden on human analysts.



📝 SOLUTION PROPOSED

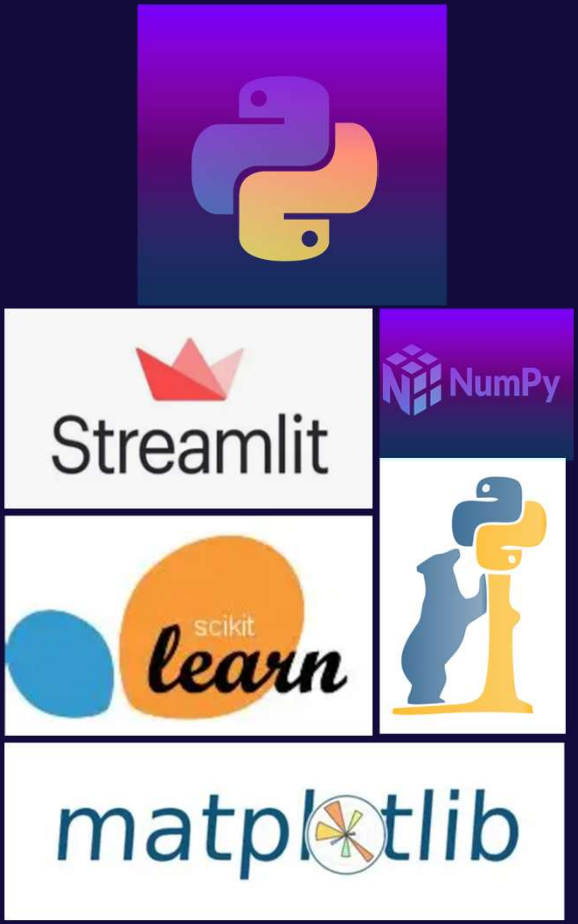
🤖 AI & Machine Learning

👉 We built a lightweight demo application using **Streamlit** that automatically analyzes log data and network events.

👉 The system **ingests raw logs**, extracts key behavioral features such as request volume, payload entropy, suspicious keywords, and URL patterns.

👉 Using an **IsolationForest machine learning model**, it identifies unusual or potentially malicious activities in real time.

👉 The tool then provides **quick remediation suggestions**, highlighting why an IP or user was flagged e.g., high suspicious URL ratio, abnormal payloads, or large request spikes.



Technology Stack Tools

- Python 3.10+ : Main Language
- Streamlit : Quick UI for demo and Deployment
- Pandas / NumPy : Data Processing
- Scikit-Learn : IsolationForest anomaly Detection
- Matplotlib : Simple Charts
- tldextract : URL Parsing and Heuristics

CONCLUSION

⚡ **AI-driven detection is essential**: Modern cyber threats are too fast and complex for human-only analysis.

🤖 Our **MVP demo** shows how lightweight AI + automation can detect anomalies, suspicious URLs, and manipulated information in real time.

📊 **Streamlit-based prototype** provides quick visualization, exportable alerts, and a judge-friendly demo flow.

🚀 **Future scope**:

- Integration with live threat intelligence feeds
- Automated incident response (blocking & notifications)
- Scalable deployment for real-world use

👉 **Key Takeaway:**

AI-powered digital security enhances speed, accuracy, and adaptability — making it a vital solution for the next generation of cyber defense.

THANK YOU

REGARDS
AI JUGAAD SQUAD