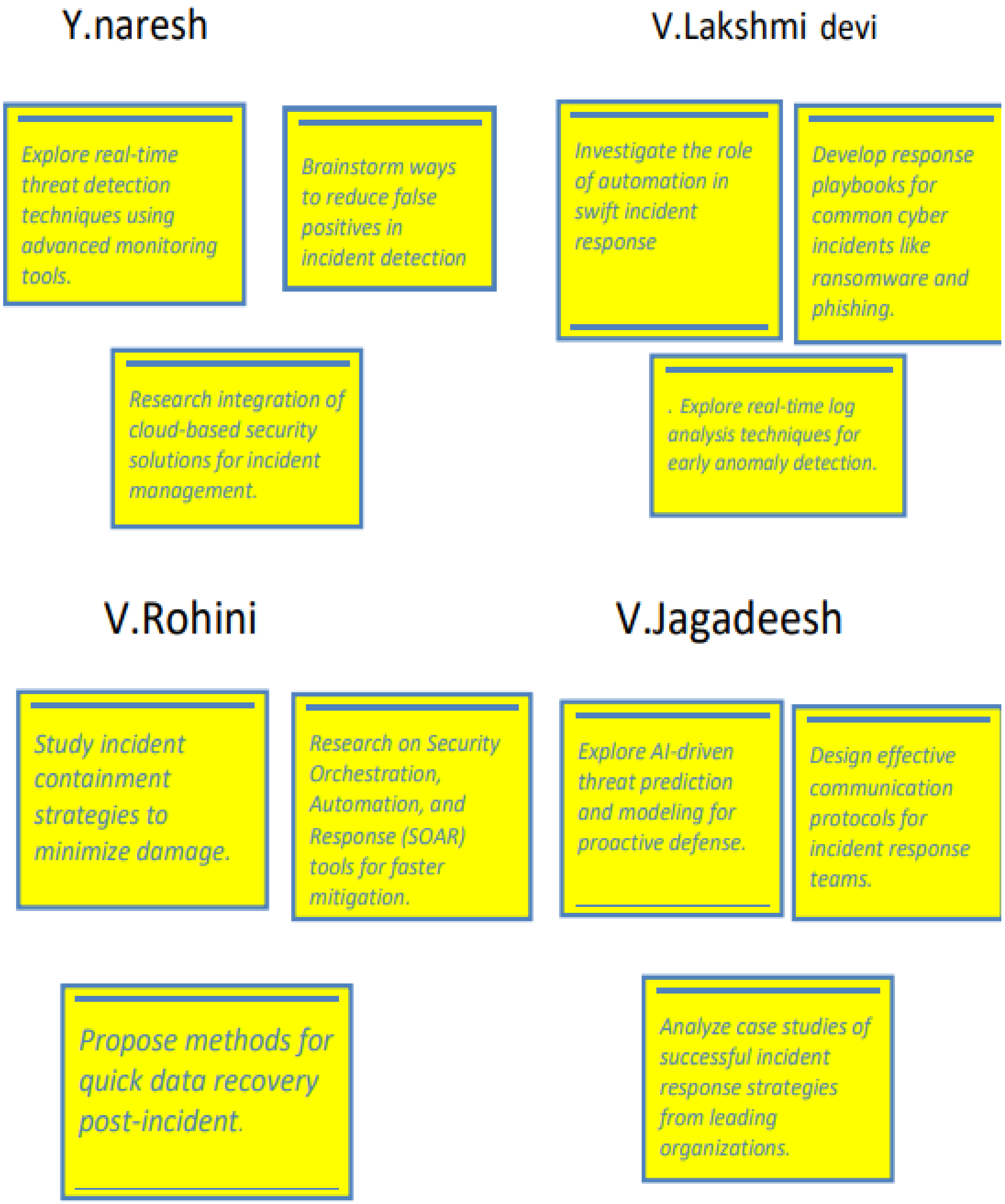
PROBLEM STATEMENT :

The Various Thoughts behind this project:



Y.naresh

Explore real-time threat detection techniques using advanced monitoring tools.

Brainstorm ways to reduce false positives in incident detection

Research integration of cloud-based security solutions for incident management.

V.Lakshmi devi

Investigate the role of automation in swift incident response

Develop response playbooks for common cyber incidents like ransomware and phishing.

. Explore real-time log analysis techniques for early anomaly detection.

V.Rohini

Study incident containment strategies to minimize damage.

Research on Security Orchestration, Automation, and Response (SOAR) tools for faster mitigation.

Propose methods for quick data recovery post-incident.

V.Jagadeesh

Explore AI-driven threat prediction and modeling for proactive defense.

Design effective communication protocols for incident response teams.

Analyze case studies of successful incident response strategies from leading organizations.