PROBLEM STATEMENT

Ideas

SHYAM RAHUL

- Tracking stolen credentials, leaked data, and hacker forums.
- Automating security assessments.
- Using CASB (Cloud Access Security Brokers) for monitoring.
- Restricting access to critical assets using network segmentation.
- Ensuring users only have permissions necessary for their role.
- Real-time exchange of cyber threat indicators.

VINAY

- Detecting patterns in security logs.
- Testing defenses against real-world attack techniques.
- Detecting anomalous behaviors and threat patterns.
- Deploying AI-powered endpoint detection & response (EDR) solutions.
- Detecting zero-day attacks based on abnormal system behavior.
- Detecting threats across endpoints and networks.

SIVA SAI

- Collaborating with industry partners for faster response
- Moving beyond signature-based detection to focus on attacker behavior.
- Using AI to analyze and predict cyber threats.
- Sharing intelligence across SOC (Security Operations Centers) and implementing preventive measures.
- Tracking stolen credentials, leaked data, and hacker forums.
- Leveraging historical attack data for better predictions.

NOHIN

- Detecting suspicious user and entity behavior (UEBA).
- Identifying malicious packets, command-and-control (C2) activity, and data exfiltration attempts.
- Deploying AI-powered endpoint detection & response (EDR) solutions.
- Strengthening authentication through biometrics, OTPs, and hardware tokens.
- Limiting admin privileges to reduce insider threats.
- Mapping attacker tactics, techniques, and procedures (TTPs).