Cloud Insider Threat Early Warning System

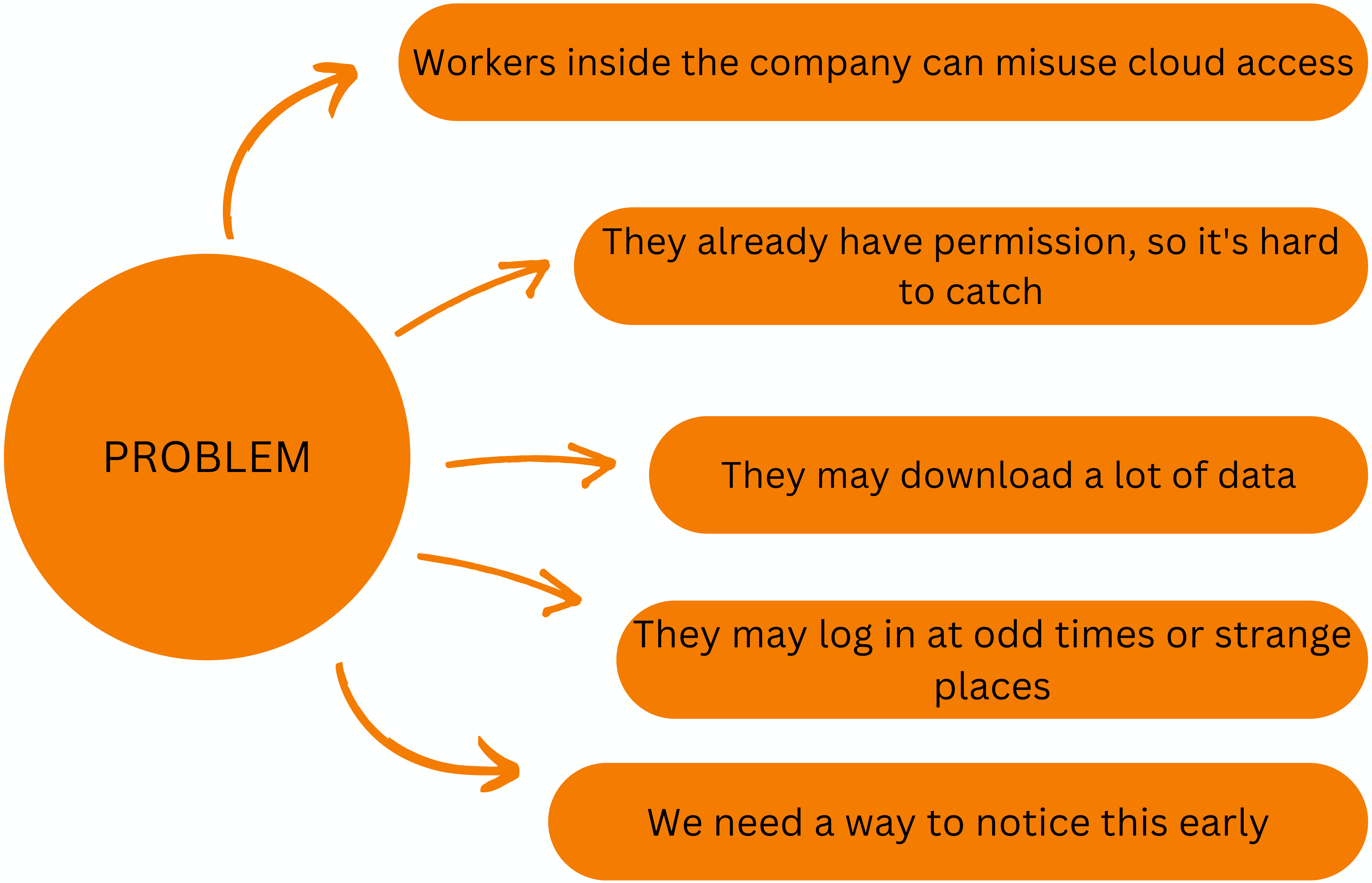
Category: Software

Theme: Cloud Security

hack-o-holics

Rashmitha.J
Ashika.S
Madhumitha Rajaraman

PROBLEM

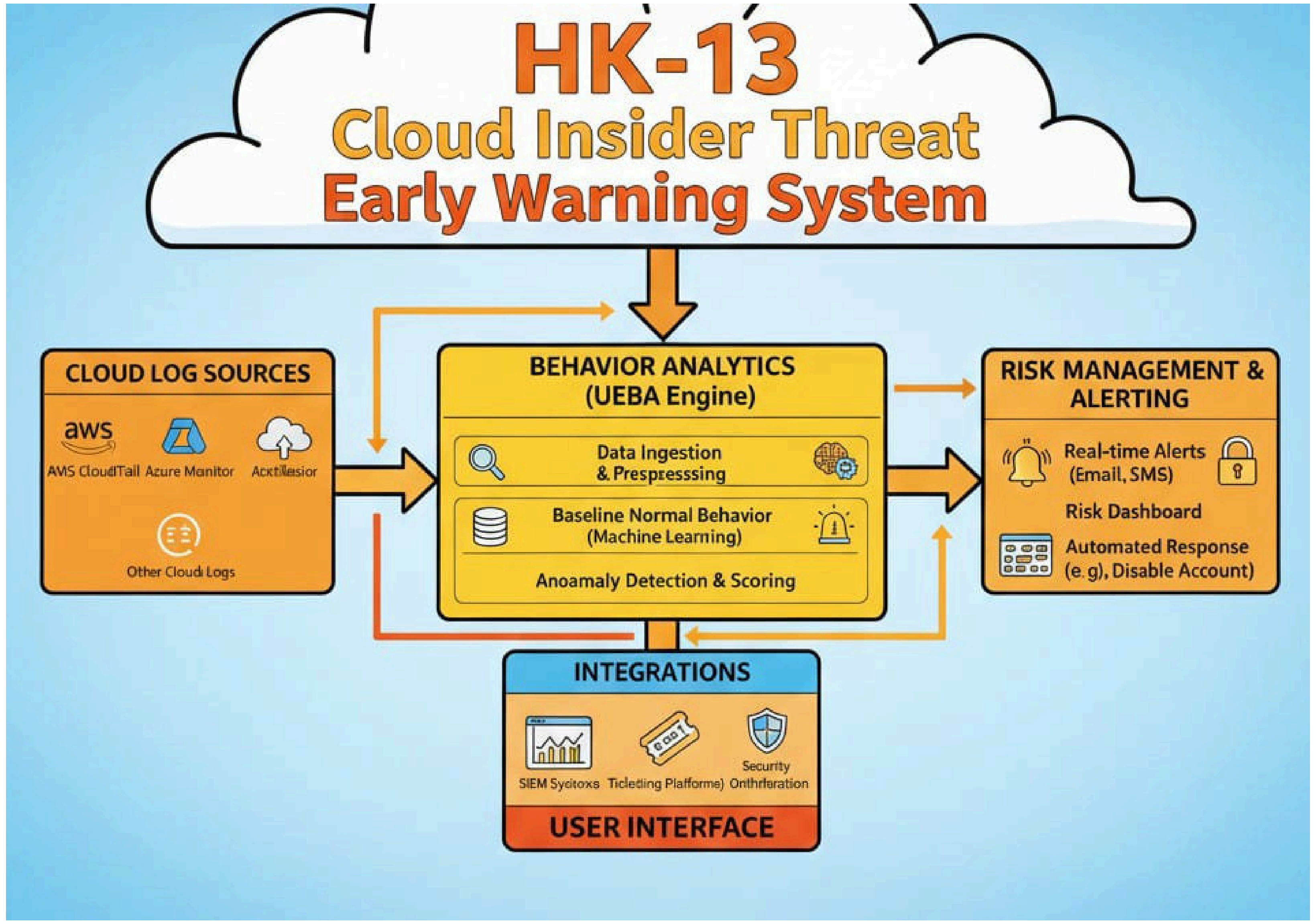


PROBLEM

- Workers inside the company can misuse cloud access
- They already have permission, so it's hard to catch
- They may download a lot of data
- They may log in at odd times or strange places
- We need a way to notice this early

SOLUTION

- Watch cloud user activities
- Learn how users normally behave
- Find unusual behavior
- Show alerts for risky actions
- Display results on a dashboard



MAIN FEATURES

- Tracks login time
- Tracks data downloads
- Tracks API calls (actions done by users)
- Checks login location
- Marks risk as low, medium or high
- Easy web dashboard

TECHNICAL OVERVIEW

Tech Stack:

Python (Backend)

Streamlit (Web Dashboard)

Pandas (Data Processing)

Plotly (Graphs & Charts)

Cloud Logs (AWS / Azure / GCP)

Workflow:

Collect cloud log data

Parse and clean data

Learn normal user behavior (baseline)

Detect unusual actions

Assign risk score (Low / Medium / High)

Show alerts on dashboard

Why This Works:

Lightweight and fast

Cloud platform independent

Easy to deploy and integrate

BENEFITS

- Helps stop data theft
- Detects harmful actions early
- Reduces manual work for security team
- Protects company cloud systems
- Simple and useful for companies

FUTURE SCOPE

- Add AI detection
- Connect to security tools
- Check location by IP
- Auto response to threats
- Support all cloud platforms

Thanya Pillai