**🚀 Problem Statement (Easy to Understand)**

**“How can we build a smart, conversational SIEM assistant that can analyze logs, detect suspicious activities, and generate tamper-proof forensic reports using NLP, while ensuring the system remains secure and private?”**

* **SIEM** = Security Information and Event Management → basically software that collects logs (records of activity) and looks for cyberattacks.
* **ISRO’s need** → They manage satellites, rockets, and ground control. If a hacker tries to break in, it will first show up in their **logs** (failed logins, suspicious IPs, malware activity). They need a smart assistant that can:
  1. **Ingest logs** (from different systems),
  2. **Detect threats**,
  3. **Explain findings clearly**,
  4. **Generate forensic reports** for investigation.

**🛡️ What Avighna2 Does Right Now**

Avighna2 is a **Conversational SIEM Assistant** — you can literally talk to it in text (or voice later) like:

[You] > ingest logs/access.log

[Avighna] Log summary: Top IPs, failed logins, suspicious entries

It’s built **offline-first** and works on **local logs/files** (safe for ISRO).

**🔹 Core Modules / Features**

**1. Log Ingestion & Parsing**

* Reads log files (e.g., access logs, system logs).
* Shows top IPs, failed logins, suspicious activity.
* If log is corrupted → it **quarantines** the log safely instead of crashing.

**2. Threat Detection Rules**

* Detects **brute-force login attempts** (too many failed logins).
* Flags suspicious IPs (foreign, repeated attackers).
* YARA scanning: checks files/logs for known malicious patterns.

**3. Enrichment**

* GeoIP Lookup → finds where an IP comes from (country, ISP).
* WHOIS / Reverse DNS → who owns the IP/domain.
* Adds context for analysts.

**4. NLP Query System**

* You can type natural queries like:
  + “show top 3 failed logins”
  + “generate report”
* Avighna understands and executes.

**5. Forensic Report Generator**

* Creates a **PDF report** with:
  + Case name
  + Findings summary
  + Evidence (logs, alerts)
  + SHA256 hash → tamper-proof integrity check
* Reports are saved in /reports/ folder.

**6. Security Systems Inside Avighna2**

* **Passcode Protection** → before running sensitive tasks (like scanning or generating reports), user must enter passcode.
* **Failed Attempts Handling** →
  + 3 wrong tries = ⚠️ Warning + beep
  + 5 wrong tries = 🔒 Lock system for 2 minutes + loud alert beep
* **Quarantine System** → corrupted/malicious logs are moved safely to logs/quarantine.
* **Alert System** → if brute-force or malware is detected → Avighna beeps + prints 🚨 warning.
* **Tamper-proof Reports** → Every PDF has a SHA256 hash (like a digital fingerprint).

**🎯 How Avighna2 Helps ISRO**

1. **Protects mission systems** → detects failed logins, suspicious IPs, unauthorized access.
2. **Monitors network logs** → can catch brute-force attempts or abnormal patterns.
3. **Investigates incidents** → generates tamper-proof forensic reports for analysts.
4. **Assists security staff** → conversational interface makes it easier to use (no need to type complex Linux commands).
5. **Privacy-first** → runs offline, doesn’t send ISRO’s data to external servers.

**🖥️ Easy Example Workflow**

1. Analyst runs Avighna2 (python -m app.Avighna2).
2. Ingests logs:
3. [You] > ingest logs/access.log

Avighna shows summary + warns if brute-force detected.

1. Checks suspicious IP:
2. [You] > geoip 8.8.8.8

Returns location + ISP.

1. Scans file:
2. [You] > scan file logs/sample.txt

Alerts if malware patterns found.

1. Generates report:
2. [You] > report
3. (asks passcode, generates PDF with SHA256 hash)

**✅ In Simple Words**

* **Problem:** Logs are huge, boring, and hard to analyze — but they contain the first signs of attacks. ISRO (and any critical org) must detect these quickly.
* **Solution (Avighna2):** A smart assistant that ingests logs, detects attacks, enriches info, alerts when needed, and generates forensic reports — all with a secure passcode system, quarantine, and tamper-proof evidence.
* **Extra:** Easy to use (conversational), offline (safe for ISRO), and systematic (alerts, reports, beeps).