**2. AI Engineer Perspective**

**Main Goal:** Develop models and automation to **enrich, correlate, and analyze threat data** for actionable insights.

**Responsibilities**

1. **Threat Data Enrichment Automation**
   * Create scripts or models to auto-query APIs for additional IOC context.
   * Use ML for:
     + **Domain classification** (malicious vs. benign)
     + **Threat actor attribution** based on patterns.
     + **Malware family classification** from hash metadata.
2. **Correlation & Scoring Models**
   * Build an IOC confidence scoring system based on:
     + Number of sources confirming the IOC
     + Reputation scores from APIs
     + Historical patterns in attacks
   * Cluster related IOCs (e.g., IP + domain + file hash).
3. **NLP for Threat Reports**
   * Process unstructured threat intel reports and extract structured IOCs using NLP (e.g., spaCy, transformers).
   * Classify text into TLP categories if not explicitly tagged.
4. **Anomaly Detection**
   * Detect **suspicious spikes** in malicious domains or IPs.
   * Identify **outliers** in IOC characteristics.
5. **Integration with Backend**
   * Work with backend engineers to serve AI/ML models via REST APIs or gRPC.
   * Ensure models are deployed in a scalable & secure way.

**Expected Outcomes**

* Automated enrichment reduces manual analyst work by **30–50%**.
* ML-driven confidence scoring improves **IOC prioritization**.
* NLP pipelines turn raw reports into **machine-usable structured data**.
* Real-time anomaly detection alerts analysts to emerging threats.

**Key Collaboration Points**

| **Role** | **Your Interaction** |
| --- | --- |
| **Backend Engineers** | Provide clean APIs for data ingestion & retrieval; work together on schema design for AI features. |
| **Security Engineers** | Get feedback on ML scoring accuracy, enrichment relevance, and IOC classification logic. |
| **DevOps** | Ensure data & model pipelines are secure, scalable, and monitored. |