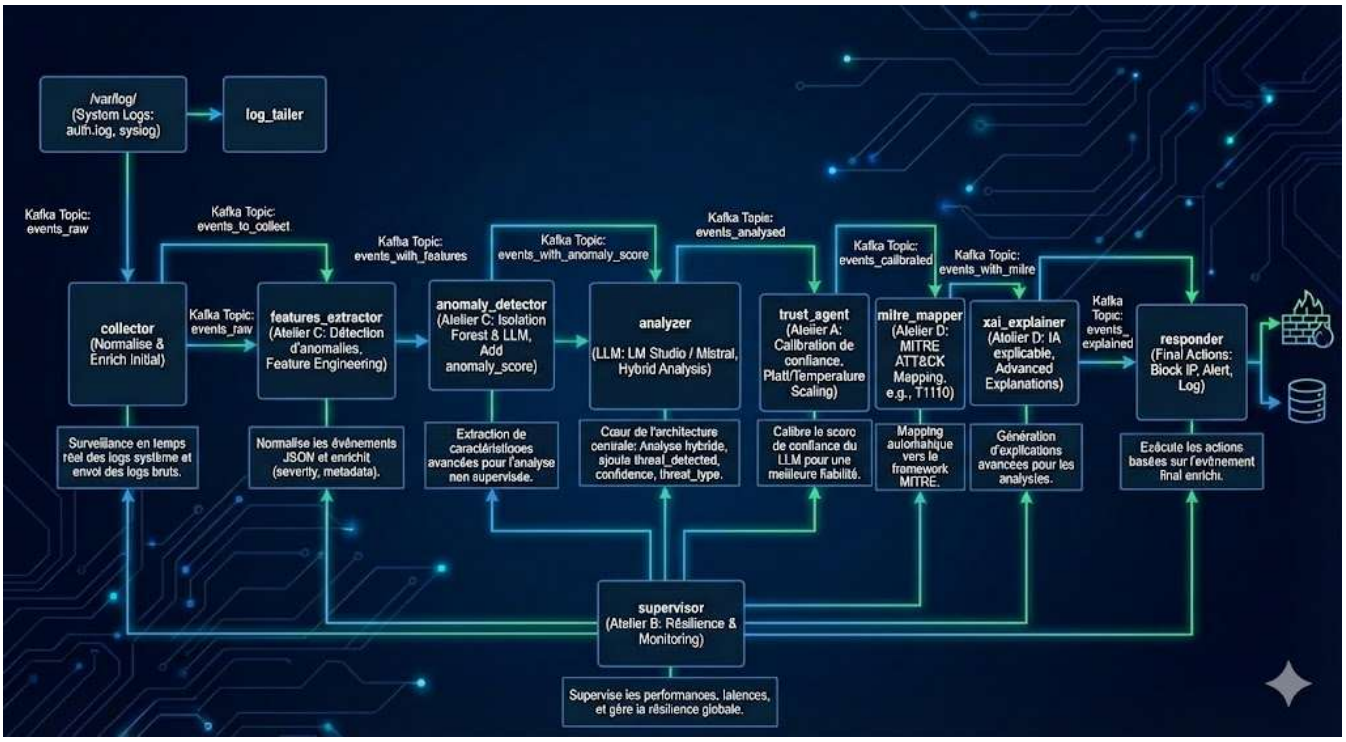
Flux détaillé du pipeline

Le traitement est **événementiel, asynchrone et distribué** via Kafka : chaque agent consomme d'un topic, enrichit l'événement JSON, et publie dans le topic suivant.



1. ***/var/log/ → log_tailer → [Kafka: events_raw]***
   - Surveillance en temps réel des logs système (auth.log, syslog, etc.).
   - Envoi des logs bruts (ou légèrement pré-traités) dans le topic raw.
2. **collector → [Kafka: events_to_collect]**
   - Normalise les événements (format JSON standardisé, extraction IP, timestamp, type, etc.).
   - Enrichissement initial (severity, metadata).
3. **features_extractor → [Kafka: events_with_features]**
   - **Contribution Atelier C** (Détection d'anomalies).
   - Feature Engineering : extraction de caractéristiques avancées (fréquences, patterns temporels, etc.) pour préparer l'analyse non supervisée.
4. **anomaly_detector → [Kafka: events_with_anomaly_score]**
   - **Atelier C**.
   - Utilise Isolation Forest (unsupervised) + pipeline hybride avec LLM.
   - Ajoute un anomaly_score à l'événement (détection de zero-day).
5. **analyzer (LLM) → [Kafka: events_analyzed]**
   - **Cœur de l'architecture centrale**.
   - Analyse hybride : heuristiques + appel à LLM local (LM Studio / Mistral).
   - Ajoute threat_detected, confidence, threat_type, recommended_action, explanation préliminaire.
6. **trust_agent (calibration) → [Kafka: events_calibrated]**

    - **Atelier A** (Calibration de confiance).
    - Applique Platt Scaling ou Temperature Scaling pour calibrer le score de confiance du LLM (rend confidence plus fiable).
7. **mitre_mapper → [Kafka: events_with_mitre]**
    - **Atelier D** (MITRE ATT&CK).
    - Mapping automatique vers le framework MITRE (ajoute mitre_technique, tactiques comme T1110 pour brute force).
8. **xai_explainer → [Kafka: events_explained]**
    - **Atelier D** (IA explicable).
    - Génération d'explications avancées (template-based via LLM ou XAI), pour rendre les décisions transparentes aux analystes.
9. **responder (actions finales)**
    - Exécute les actions : blocage IP (iptables), alertes, logging.
    - Basé sur l'événement final enrichi (haute confiance, MITRE, explication).
10. **supervisor (monitoring)**
    - **Atelier B** (Résilience).
    - Supervise les performances, latences, pannes (intégration avec le supervisor de l'atelier B).
    - Gère la résilience globale (détection surcharge, redémarrage composants).

Avantages de cette architecture intégrée

- **Distribution via Kafka (Atelier B)** : Découplage total, résilience (replay en cas de panne), scalabilité horizontale.
- **Précision et fiabilité** : Anomalies (C) + Calibration (A).
- **Explicabilité** : Mapping MITRE + XAI (D).
- Tout reste **local** (LLM via LM Studio), sans **cloud**.

Voici la **trace complète** d'un événement unique traversant l'intégralité du pipeline, de l'extraction brute jusqu'à l'action finale.

Le JSON s'enrichit étape par étape. Les nouveaux champs ajoutés à chaque étape sont commentés.

1. Source & Log Tailer (Entrée Brute)

Topic Kafka : `events_raw` L'agent capture une ligne dans `/var/log/auth.log`.

```
{
  "timestamp": "2025-01-03T15:30:00Z",
  "source": "/var/log/auth.log",
  "host": "server-ubuntu-01",
  "message": "Failed password for admin from 192.168.1.100 port 52341 ssh2"
}
```

2. Collector (Normalisation)

Topic Kafka : `events_to_collect` L'événement est standardisé. Les IPs et utilisateurs sont extraits via Regex.

```
{
    "event_id": "evt_1735915800000",
    "timestamp": "2025-01-03T15:30:00Z",
    "source": "/var/log/auth.log",
    "ip_source": "192.168.1.100",
    "severity": "high",
    "metadata": {
        "collector_id": "collector_001",
        "extracted_info": {
            "event_type": "auth_failure",
            "protocol": "ssh",
            "user": "admin"
        }
    },
    "raw_message": "Failed password for admin..."
}
```

3. Features Extractor (Atelier C - Engineering)

Topic Kafka : `events_with_features` Préparation pour l'IA non supervisée. Transformation des données en caractéristiques numériques.

```
{
    "event_id": "evt_1735915800000",
```

```
    // ... champs précédents conservés ...
    "features": {
        "ip_entropy": 0.45,
        "time_hour_sin": -0.707, // Heure encodée cycliquement
        "failed_count_5min": 12, // Fréquence calculée
        "is_root_attempt": 0,
        "packet_size": 128
    }
}
```

4. Anomaly Detector (Atelier C - Isolation Forest)

Topic Kafka : `events_with_anomaly_score` L'Isolation Forest évalue si cet événement est rare ou aberrant.

```
{
    "event_id": "evt_1735915800000",
    // ... champs précédents ...
    "anomaly_analysis": {
        "score": 0.85, // Score proche de 1 = anomalie forte
        "is_anomaly": true,
        "algorithm": "isolation_forest_v2",
        "threshold": 0.70
    }
}
```

5. Analyzer (Analyse Hybride & LLM)

Topic Kafka : `events_analyzed` Le LLM analyse le contexte + le score d'anomalie pour qualifier la menace.

```
{
    "event_id": "evt_1735915800000",
    // ... champs précédents ...
    "analysis": {
        "threat_detected": true,
        "threat_type": "ssh_bruteforce",
        "initial_confidence": 0.95, // Confiance brute du LLM
        "reasoning": "Multiples échecs suivis d'un score d'anomalie élevé (0.85).
Pattern typique de force brute."
    }
}
```

6. Trust Agent (Atelier A - Calibration)

Topic Kafka : `events_calibrated` Calibration mathématique (Platt Scaling) pour rendre la confiance réaliste (évite l'overconfidence du LLM).

```
{
    "event_id": "evt_1735915800000",
    // ... champs précédents ...
    "trust_calibration": {
        "raw_confidence": 0.95,
        "calibrated_confidence": 0.88, // Score ajusté et plus fiable
        "method": "platt_scaling",
        "reliability_group": "high"
    }
}
```

7. MITRE Mapper (Atelier D - Contextualisation)

Topic Kafka : `events_with_mitre` Mapping automatique vers le framework MITRE ATT&CK.

```
{
    "event_id": "evt_1735915800000",
    // ... champs précédents ...
    "mitre_attack": {
        "technique_id": "T1110",
        "technique_name": "Brute Force",
        "tactic": "Credential Access",
        "url": "https://attack.mitre.org/techniques/T1110/"
    }
}
```

8. XAI Explainer (Atelier D - Explicabilité)

Topic Kafka : `events_explained` Génération d'une explication en langage naturel pour l'analyste humain.

```
{
    "event_id": "evt_1735915800000",
    // ... champs précédents ...
    "explanation": {
        "summary": "Attaque par force brute confirmée sur le compte admin.",
        "key_factors": [
            "Fréquence élevée",
            "Score anomalie > 0.8",
            "Mot clé 'Failed'"
```

```
        ],
        "human_message": "L'IP 192.168.1.100 tente de forcer l'accès. Confiance
calibrée de 88%. Action de blocage recommandée."
    }
}
```

9. Responder (Action Finale)

Action exécutée sur le système L'agent lit le JSON final, voit `threat_detected: true` et `confidence > 0.8`, et déclenche l'action.

```
{
    "event_id": "evt_1735915800000",
    "final_status": "closed",
    "action_taken": {
        "type": "block_ip",
        "target": "192.168.1.100",
        "tool": "iptables",
        "timestamp": "2025-01-03T15:30:05Z",
        "success": true
    }
}
```