**2. Collection – Data Sources Flowchart**

**Internal Data Sources:**

* Email gateway logs (e.g., spam filters, quarantine actions)
* SIEM logs
* EDR (Endpoint Detection & Response) telemetry
* Firewall and proxy logs
* User-reported phishing emails (via SOC/helpdesk)

**External Data Sources:**

* Threat intelligence feeds (e.g., commercial, open source)
* ISAC sector-specific sharing (e.g., H-ISAC)
* CERT/CSIRT alerts
* OSINT (e.g., pastebin, social media leak monitors)

**Output:** Raw indicators (IOCs), metadata, behavior traces collected for further processing.