# Agentic AI Architecture for SOC Operations in Cybersecurity

Multi-Agent Framework for Next-Gen Threat Detection & Response

# 1. Agent Overview

- • Threat Intelligence Agent – Correlates threat intel with internal data
- • Log Ingestion Agent – Parses and normalizes logs
- • Anomaly Detection Agent – Detects outliers using ML
- • Alert Prioritization Agent – Ranks alerts based on risk and context
- • Response Automation Agent – Executes SOAR playbooks

# 2. System Architecture Layers

- ◆ Data Layer: SIEM, EDR, threat intel, Kafka, ElasticSearch
- ◆ Agent Framework Layer: CrewAI, LangGraph, Vector DB
- ◆ Processing & Orchestration Layer: Real-time event processor, LLM core
- ◆ Response Layer: SOAR playbooks, escalation engine, audit logs

# 3. Security & Governance

- • RBAC enforcement across agents
- • Agent output validation and traceability
- • Compliance modules (GDPR, NIST)
- • Continuous feedback and learning loops

# 4. Agent Interaction Example: Phishing Email Detection

- 1. Log Ingestion Agent parses email logs
- 2. Anomaly Detection Agent flags behavior
- 3. Threat Intel Agent matches IOCs
- 4. Alert Prioritization Agent scores the alert
- 5. Response Automation Agent isolates endpoint
- 6. Human Collaboration Agent sends summary
- 7. Learning Agent updates models

# 5. Tooling Recommendations

- • LLMs: GPT-4o, Claude 3, private LLMs via Ollama
- • Vector DB: FAISS, ChromaDB for RAG
- • Agent Frameworks: CrewAI, LangGraph, AutoGen
- • Orchestration: Airflow, LangGraph
- • Dashboards: Kibana, Grafana