AI Driven SOC-In-A-Box (SOCBOX)

Data Sources

Elastic Endpoint | Syslog | Threat Feeds (MISP, OTX)

Data Processing Layer

Logstash + Elasticsearch

AI-Driven Analysis & Detection Layer

ML Models | Kibana AI | Behavioral Analytics

Incident Response and Automation Layer

TheHive | Cortex | Elastic SIEM

Threat Simulation

Infection Monkey

Atomic Red Team

Malware Anaalysis

Cuckoo Sandbox

Threat Intelligence and Collaboration Layer

MISP + External Threat Exchange

Monitoring and Visualization

Kibana + Elastic SIEM