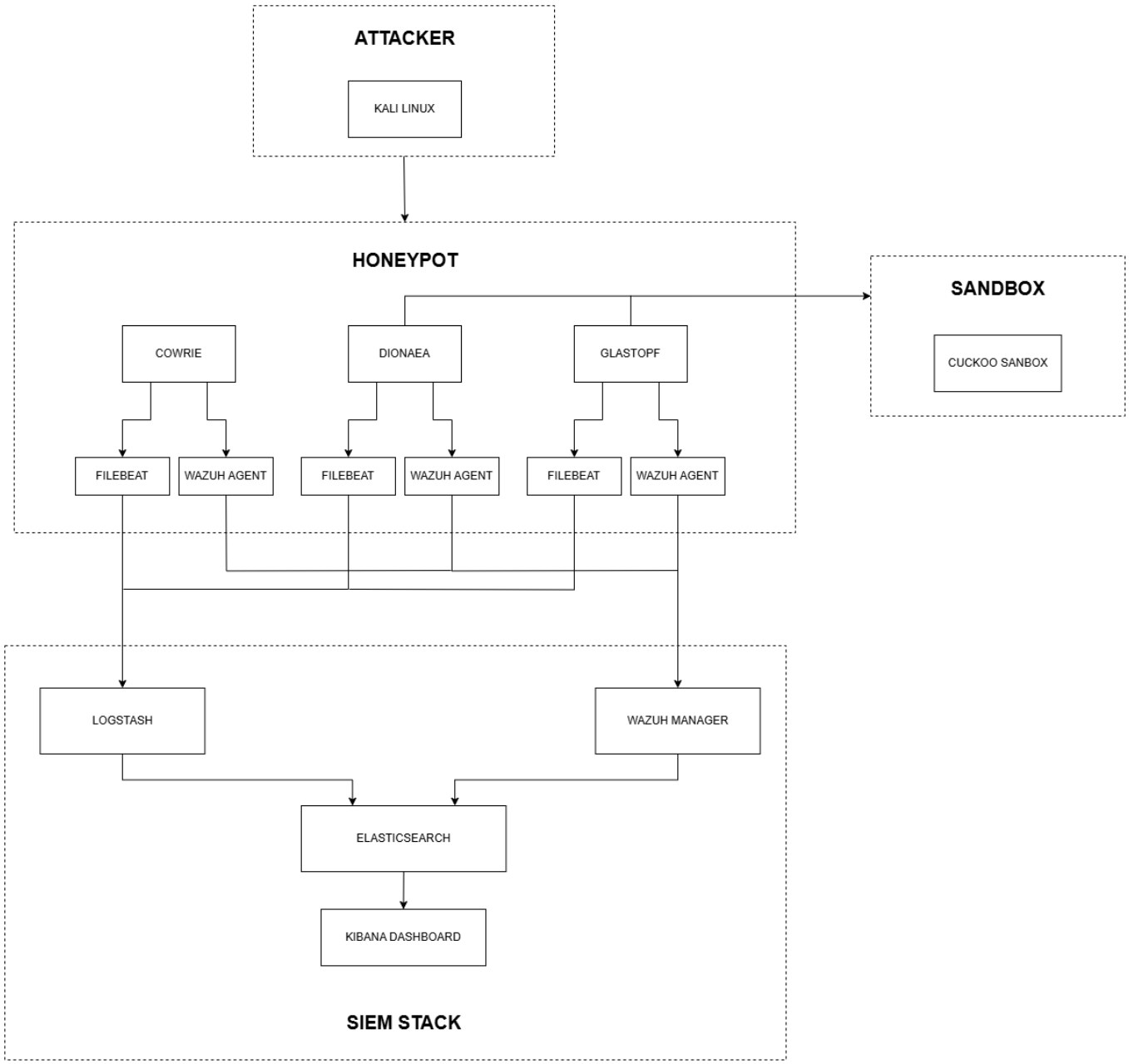
HONEYPOT SYSTEM ARCHITECTURE - DOCUMENTATION

1. Honeynet Architecture

The honeynet system is composed of multiple virtual machines (VMs) running in a controlled lab environment. The attacker, honeypot sensors (Cowrie, Dionaea, Glastopf), sandbox (Cuckoo), and SIEM stack (ELK + Wazuh) communicate over an internal network, with optional Host-only adapters for management access from the physical host.



2. Virtual Machine Operating Systems

- Honeypot 1: Ubuntu Server 20.04 LTS - Cowrie (SSH/Telnet Honeypot)

- Honeypot 2: Debian 11 (Bullseye) or Ubuntu 20.04 - Dionaea (Malware Honeypot)
- Honeypot 3: CentOS 7 or Ubuntu 18.04 - Glastopf (Web Honeypot)
- Sandbox: Windows 10 x64 (Build 21H2) - Cuckoo Sandbox (Malware Analysis)
- ELK Stack: Ubuntu Server 22.04 LTS - Elasticsearch + Logstash + Kibana
- Wazuh Server: Ubuntu Server 22.04 LTS - Wazuh Manager + API + Kibana Plugin
- Attacker: Kali Linux 2023.4 - Red Team Simulation (metasploit, nmap, sqlmap)

3. Network Configuration

The system uses the following VirtualBox network setup:

- honeynet-int (Internal Network): Communication between honeypot VMs, ELK, Wazuh, Sandbox.
- internet-nat (NAT): Optional, only for the Cuckoo guest VM to access Internet for C2 traffic.
- mgmt-hostonly (Host-only): Management access from host to guest VMs.

Each VM has Adapter 1 on 'honeynet-int' and optionally Adapter 2 on 'mgmt-hostonly' or 'internet-nat'.