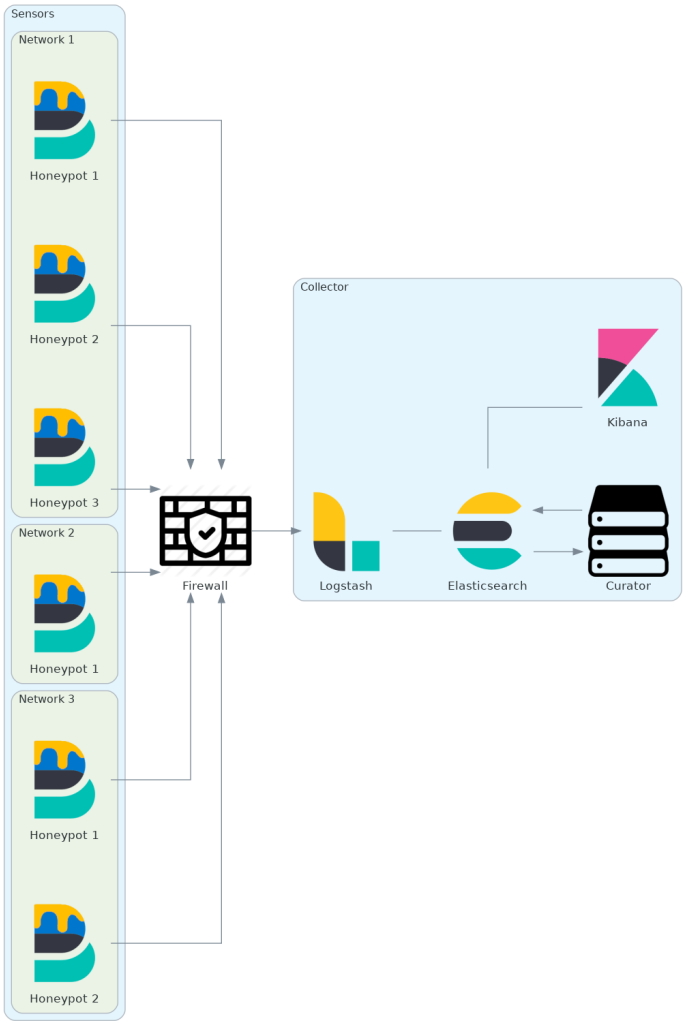
dpot

> A centralized but distributed honeypot system inspired by `telekom-security/tpotce`

Introduction

Based on the T-Pot Honeypot framework, this projects makes it easy to deploy and monitor a distributed honeypot infrastructure.

Infrastructure:



dpot Infrastructure

Collector 🍯

Components:

- ELK Stack
- Elastic Curator

Installation

1. Set your username and password in `.env` file
2. Generate certificates for Logstash and Filebeat (sensors) with `generate.sh`
3. `$ docker-compose up -d`

Sensor 🐝

Components:

- Filebeat
- Cowrie
- Mailhoney
- ElasticPot
- Dionaea / Heralding
- Suricata

Installation:

1. Set collector IP/FQDN and sensor name in `.env` file
2. Copy `ca.crt`, `ca.key` and `serial` file from logstash ssl config into `sensor/filebeat/ssl/`
3. Generate Filebeat certificate with `generate.sh`
4. Select honeypots to active by commenting the services in `docker-compose.yml` file or with `docker-compose up -d filbeat [honeypots]`
