TLS for Chipper

TLS / Encryption

- **TLS** is terminated by each instance of `fluentd`. First we need a certificate authority. Then we use this **CA** to generate the certificates that will be injected into `fluentd`. These files are located at `./server/k8s/helm/fluentd/tls`.
- As of this writing, `rsa` keys, not `ecsda` works with `fluentd`.

1. Create default CSR for your **CA**. **Make changes once it's generated**:

```
cfssl print-defaults csr > ./tls/ca-csr.json
```

2. Generate **CA** certificate and key:

```
cfssl gencert -initca ./tls/ca-csr.json | cfssljson -bare ./tls/chipper-ca
```

3. Generate certificate and key for each application to use:

```
# fluentd
echo '{"key":{"algo":"rsa","size":4096}}' | cfssl gencert -ca=./tls/chipper-ca.pem

# wazuh. and it copies certs/keys to chart directories
echo '{"key":{"algo":"rsa","size":4096}}' | cfssl gencert -ca='./tls/chipper-ca.pem
```