Detective Controls

Collecting and analyzing [audit] logs is useful for a variety of different reasons. Logs can help with root cause analysis and attribution, i.e. ascribing a change to a particular user. When enough logs have been collected, they can be used to detect anomalous behaviors too. On Amazon EKS, the audit logs are sent to Amazon Cloudwatch Logs.

For more details on various Amazon EKS Best Practices in Detective Controls, refer to the [documentation](https://aws.github.io/aws-eks-best-practices/security/docs/detective/).