Proactive Monitoring

Any system, application and (cloud) service that is in scope of GDPR should generate a log and alert:

- ❑ First time application usage by a user
- ❑ Access to configuration files that contain hard coded credentials/certificates/API keys
- ❑ Creation, activation and usage of a "guest" account
- ❑ Administrative actions if a user is added to a local admin group
- ❑ Failed login attempts of system admin accounts
- ❑ Usage of privileged accounts
- ❑ Changes to code on production systems through unauthorized procedures / at unusual times / by unknown users

**Information extracted from ICO penalty notice case ref: COM0783342*
https://ico.org.uk/media/action-weve-taken/mpns/2618421/ba-penalty-20201016.pdf