REPUDIATION OF ACTION

How hard is it for users to deny performing an action? What evidence does the system collect to help you to prove otherwise? Non-repudiation refers to the ability of a system to ensure people are accountable for their actions.

An example of repudiation of action is where a user has deleted some sensitive information and the system lacks the ability to trace the malicious operations.

KEY CONCEPTS:

- Non-Repudiation
- Logging
- Audit
- Signing

Examples of insufficient logging

- Lack of logging showing user access to sensitive data
- Lack of logging sensitive user actions, such as delete account
- Lack of logging of administrative activities
- Lack of logging of session management or authentication failures
- Lack of logging of validation errors
- Lack of centralisation of logs to a central store
- Lack of audit log showing user actions within delivery infrastructure

Examples of logs being vulnerable to tampering

- Lack access control on log files allowing attackers to cover tracks
- Lack of integrity signatures on logs for sensitive actions
- Lack of integrity signatures on artefacts passing through delivery pipeline

Examples of weakness in process

- Lack awareness of audit and access policy
- Lack of awareness material to communicate audit and abuse policy to user
- Lack of operational process or team to respond to suspicious events

And what else?