Let’s level set on Separation of Duties…

The intention

The intention behind SoD is to prevent error, abuse, or malice from single actors by disseminating tasks and privileges among multiple people.

This way no one person can make changes without some level of approval and transparency.

Detailed in security frameworks like…

- NIST 800-53
- ISO 27001
- Sarbanes Oxley (SOX)
- PCI DSS

Let’s level set on Separation of Duties…

The Reality

Frustratingly, this has become entrenched into a separation between functions and teams…

You wrote it, but someone else is responsible for:

- Testing it
- Securing it
- Deploying it
- Running it
- etc.

Each functional team locally optimizing only for the things they are responsible for, instead of optimizing the entire system.