

 **Why we are NOT doing
CI/CD today?**



- CI/CD without security is dangerous.
- First, we secure access between GitHub and GCP.
- Today's goal: secure foundation, not automation.
- A strong base avoids confusion in later videos.



 **What does
IAM actually mean?**



- IAM = Identity and Access Management.
- It controls who can do what in GCP.
- IAM is the gatekeeper of your cloud resources.
- Without IAM, cloud security is impossible.





What is an Identity?



- Identity means who is making the request.
- It can be a user, service account, or system.
- GitHub Actions is also an identity.
- GCP always checks identity before allowing access.





What are Permissions and Roles?



- Permission = a single action (example: deploy, read, write).
- Role = a collection of permissions.
- Roles make permission management easier.
- You never assign permissions directly in real projects.





Least Privilege Rule

(Golden Rule)



- Give only the permissions that are required.
- Never give admin access by default.
- Less access = less damage if something breaks.
- This rule is followed in real companies.





Old Method

Why Service Account Keys are bad?



- Keys are long-lived and dangerous.
- If a key leaks, anyone can access your cloud.
- Keys are often committed by mistake.
- Modern companies avoid keys completely.



 **Modern Method**
Workload Identity Federation



- No keys, no passwords.
- Access is temporary and secure.
- GitHub proves its identity using OIDC.
- GCP trusts GitHub only for specific actions.



 **Understand the Simple Flow**
(No technical jump)





**What is today's
RESULT?**





Industry Reality

