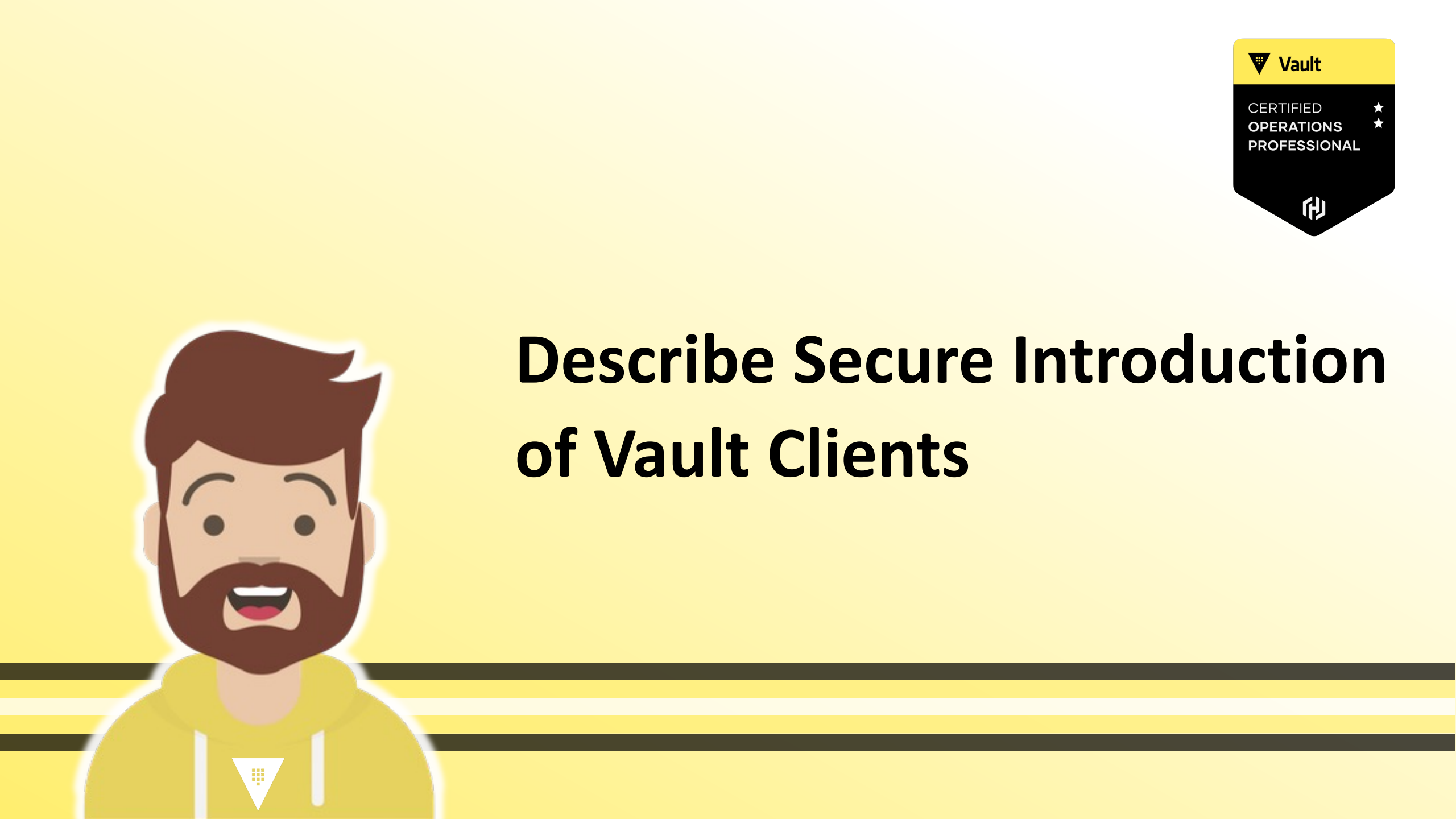


Describe Secure Introduction of Vault Clients

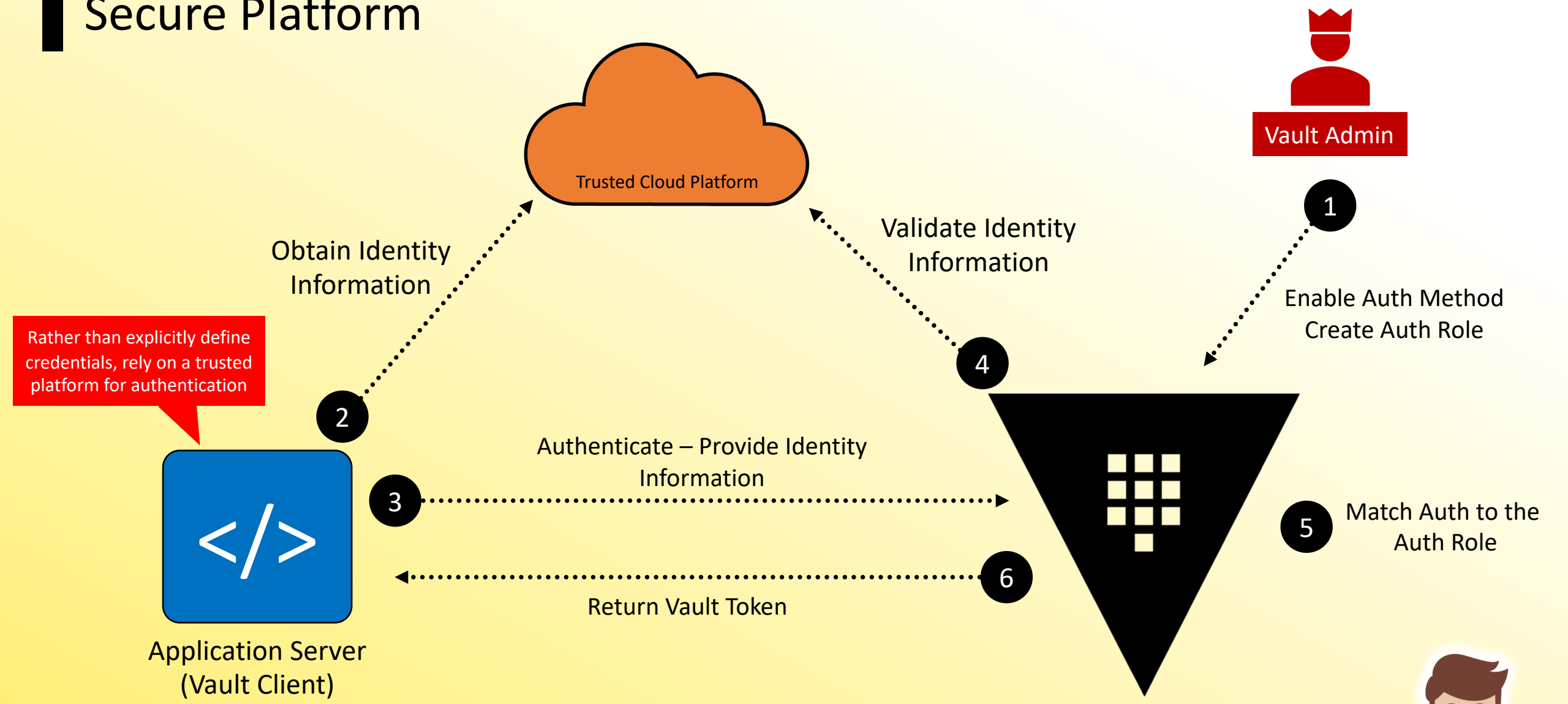
What is Secret Zero?

- Secret zero is essentially the "first secret" needed to obtain other secrets
  - Example: 1Password or LastPass
- In Vault, this is either the authentication credentials or a Vault token
- Once we have secret zero, we can potentially obtain other credentials. Unfortunately, it also allows for an unauthorized user to elevate privileges in the organization
- The goal is to introduce secret zero in the most secure fashion but only when it's needed for the application to use it

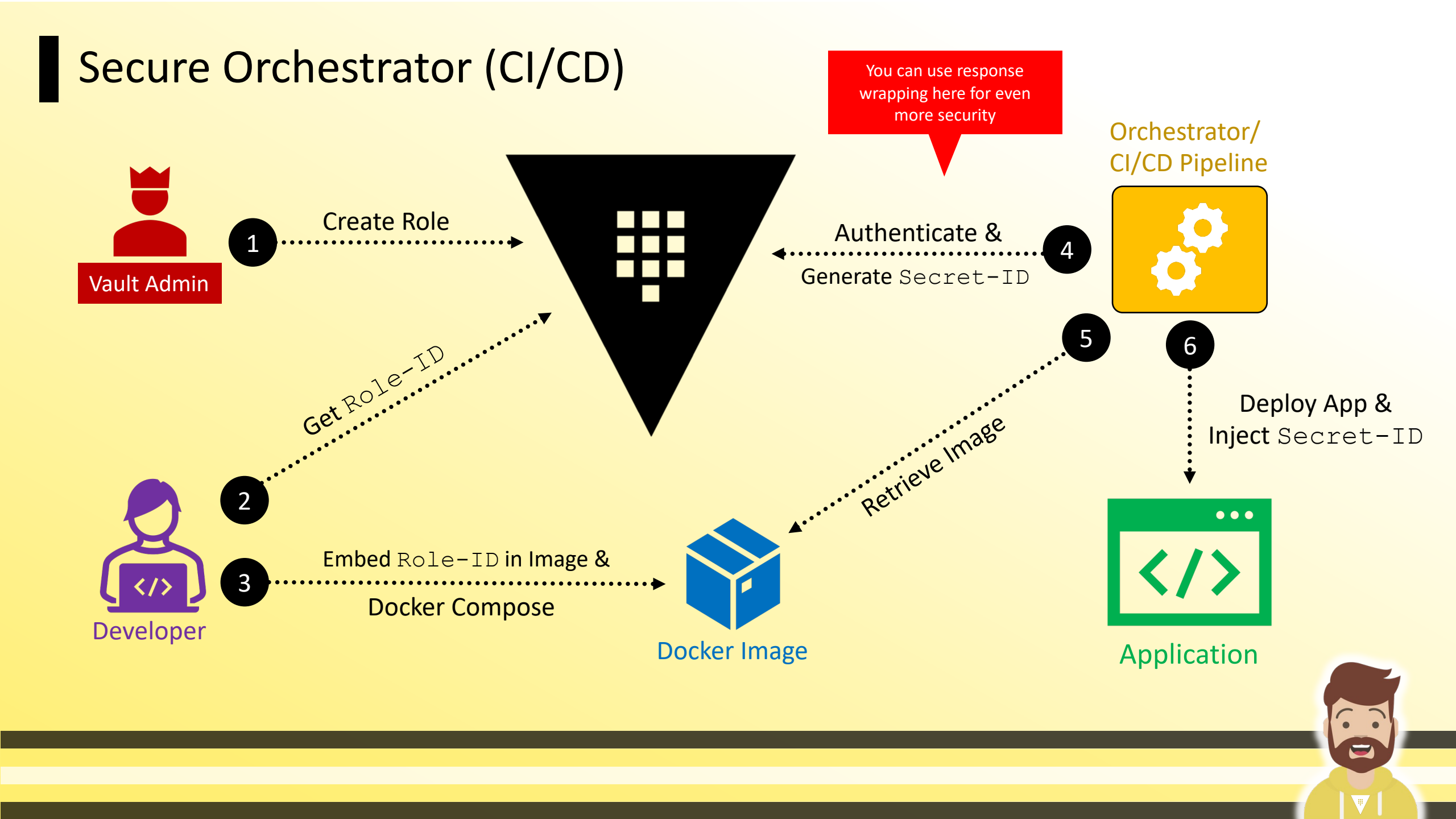
Secure Introduction Goals

1. Use unique credentials for each application instance provisioned
2. Limit your exposure if a credential is compromised
3. Stop hardcoding credentials within the application codebase
4. Reduce the TTL of the credentials used by applications and reduce long-lived creds
5. Distribute credentials securely and only at runtime
6. Use a trusted platform to verify the identities of clients
7. Employ a trusted orchestrator that is already authenticated to Vault to inject secrets

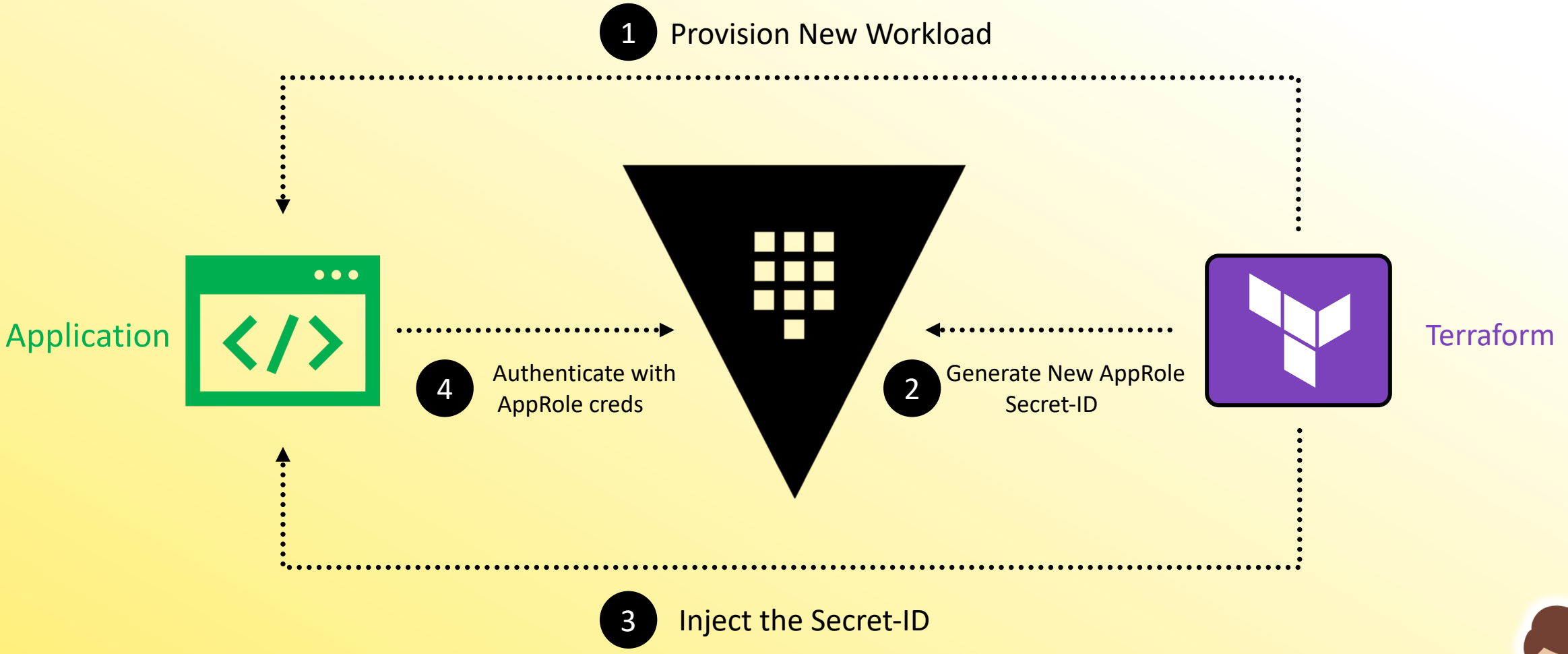
Secure Platform



Secure Orchestrator (CI/CD)



Secure Orchestrator (Terraform)



Vault Agent – Auto Auth