Mehdi LARUELLE
@D2SI

Be secret like a ninja with Hashicorp Vault

Whoami ?

D2SI

aws partner network
Training Partner

aws partner network
Premier Consulting Partner

aws 300 CERTIFIED
AWS PARTNER NETWORK

AWS User Group PARIS, FR

HashiCorp User Group PARIS

Me

Mehdi LARUELLE
Cloud & Automation
@mehdilaruelle

Github Access

Table of contents

1 Contextualization

2 How does Vault work ?

3 Steps to become a ninja

4 Demonstration

1 // Contextualization

Problem ?

Mail

Hello,

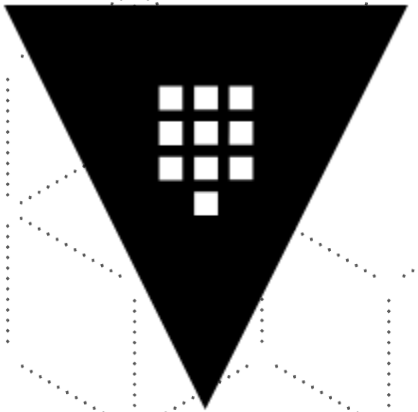
Here your access to your DB:

- Username: [redacted]
- Password: [redacted]

Code

```
$host   = getenv('DB_HOST');
$dbname = getenv('DB_NAME');
$user   = getenv('DB_USER');
$pass   = "dev";
```

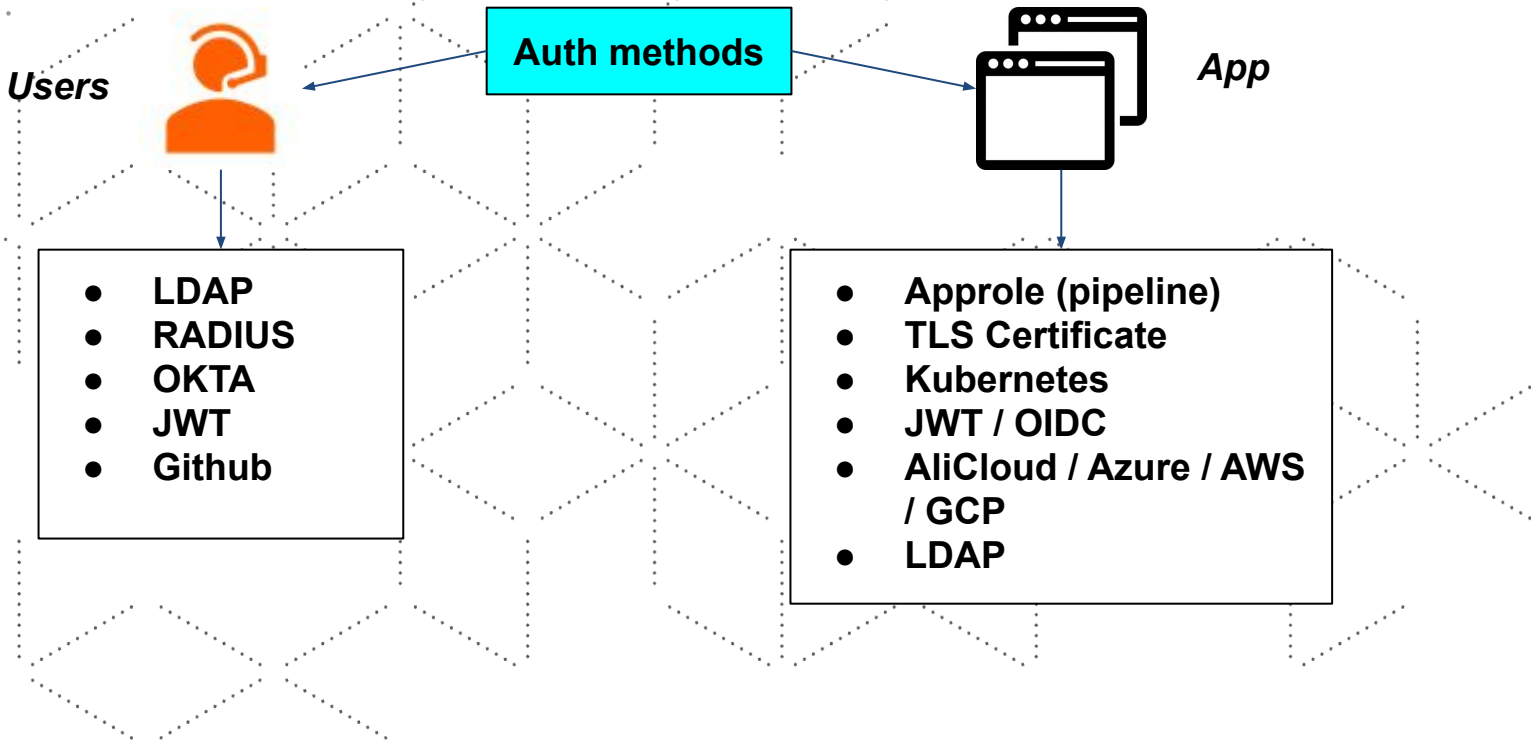
Vault ? Why ?



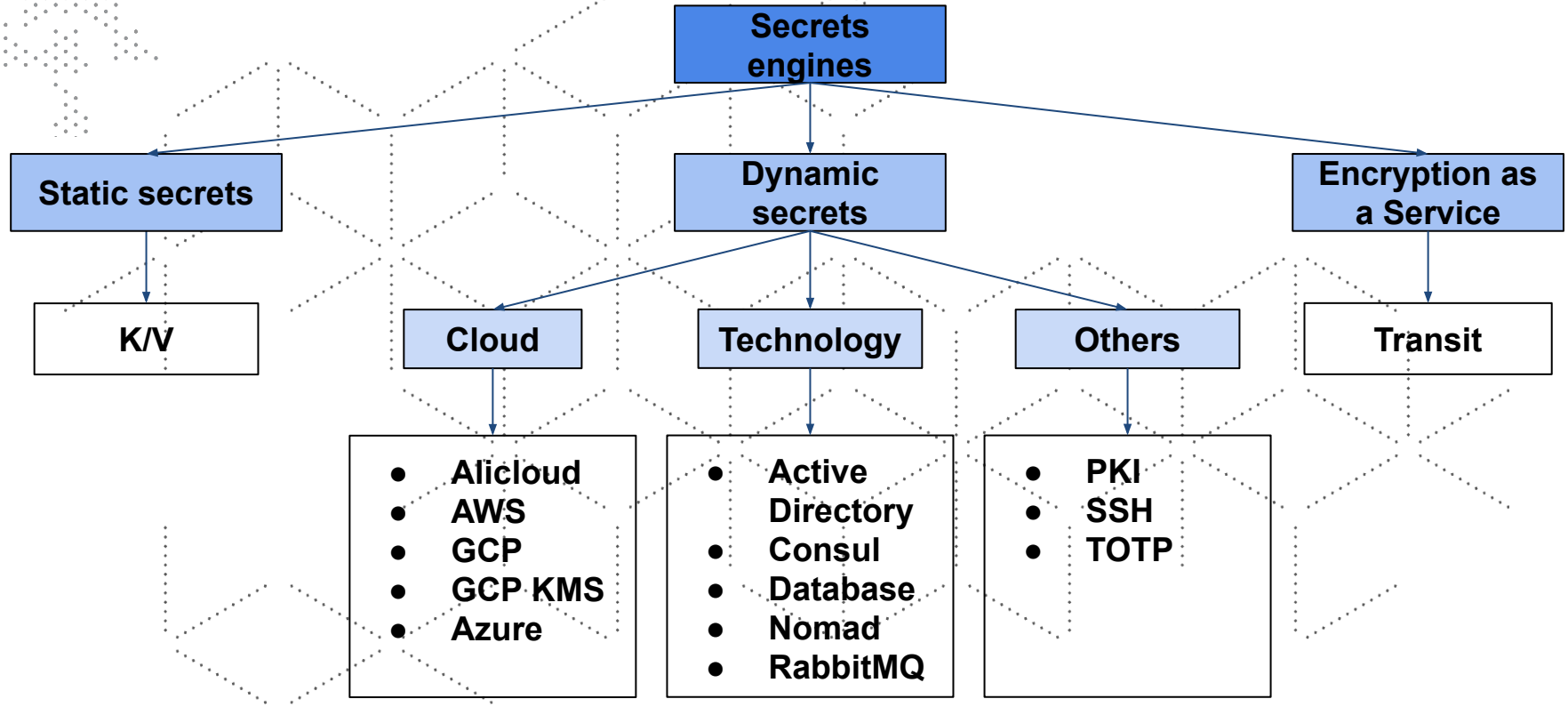
HashiCorp
Vault

2 // How does Vault work ?

Methods & Engines

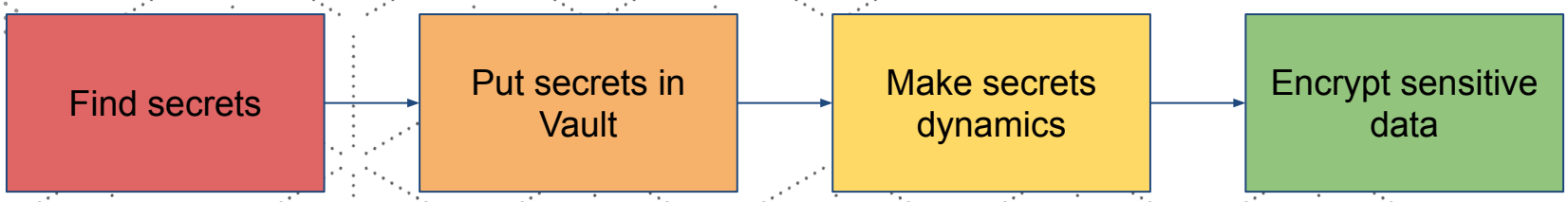


Methods & Engines

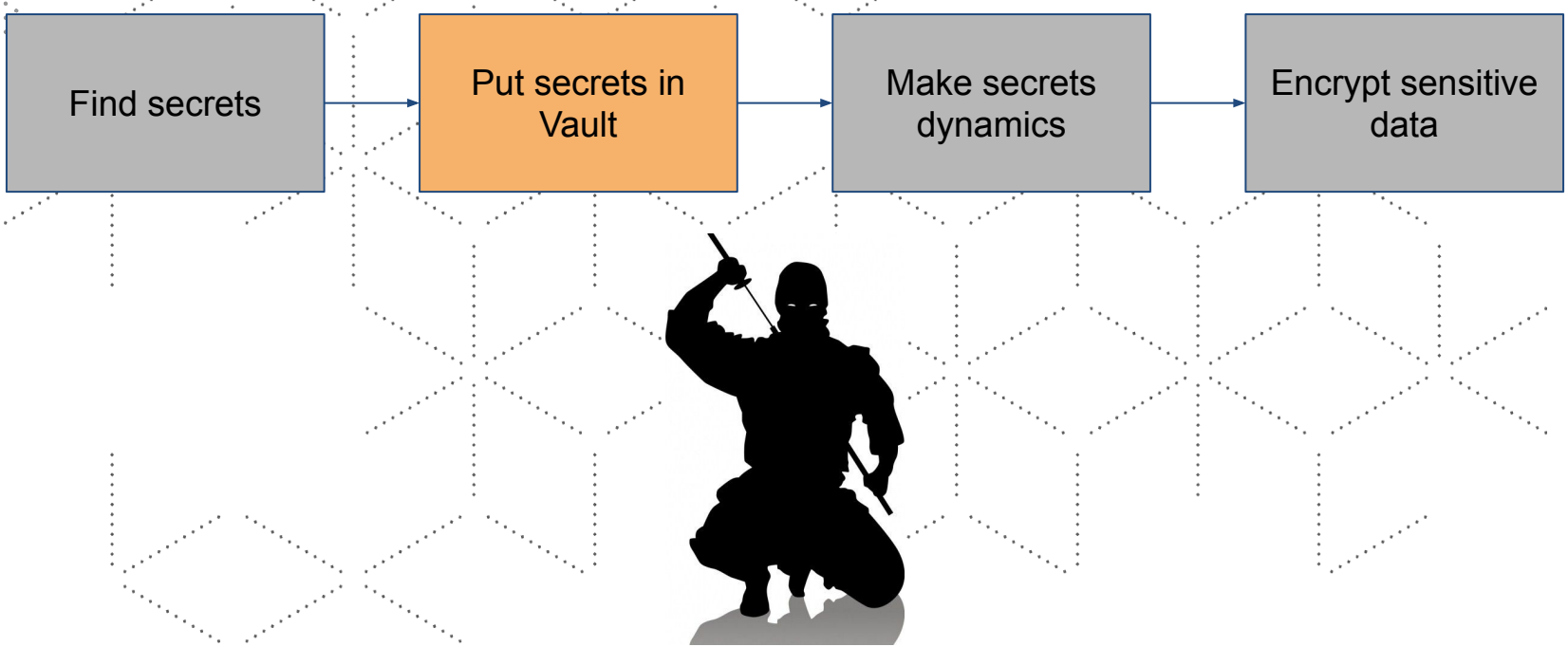


3 // Steps to become a ninja

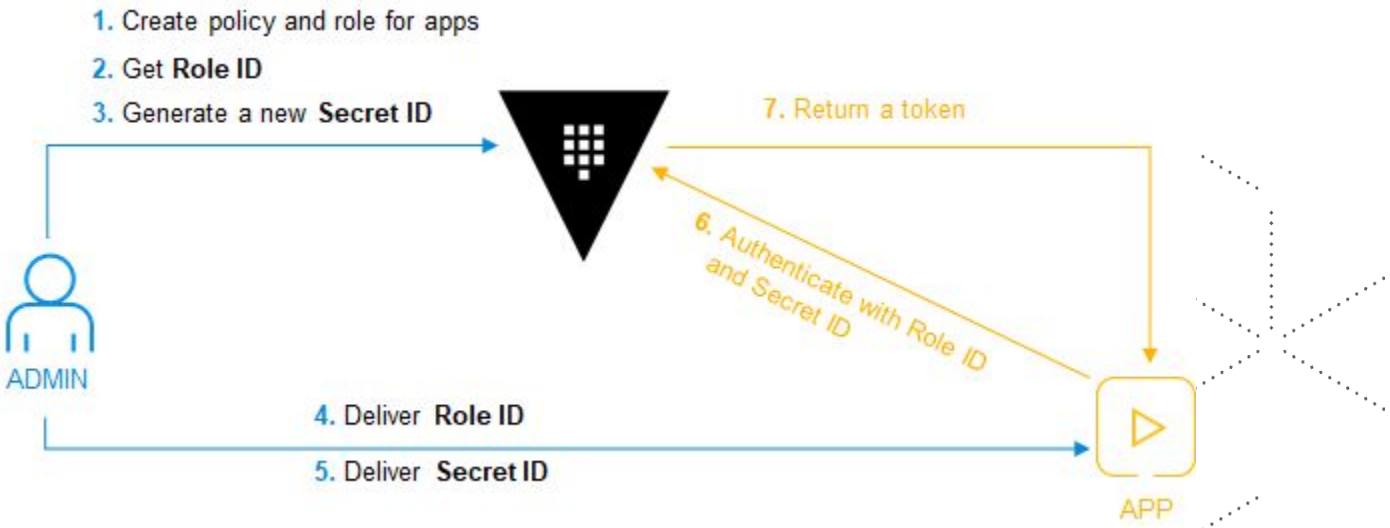
Steps to be a ninja



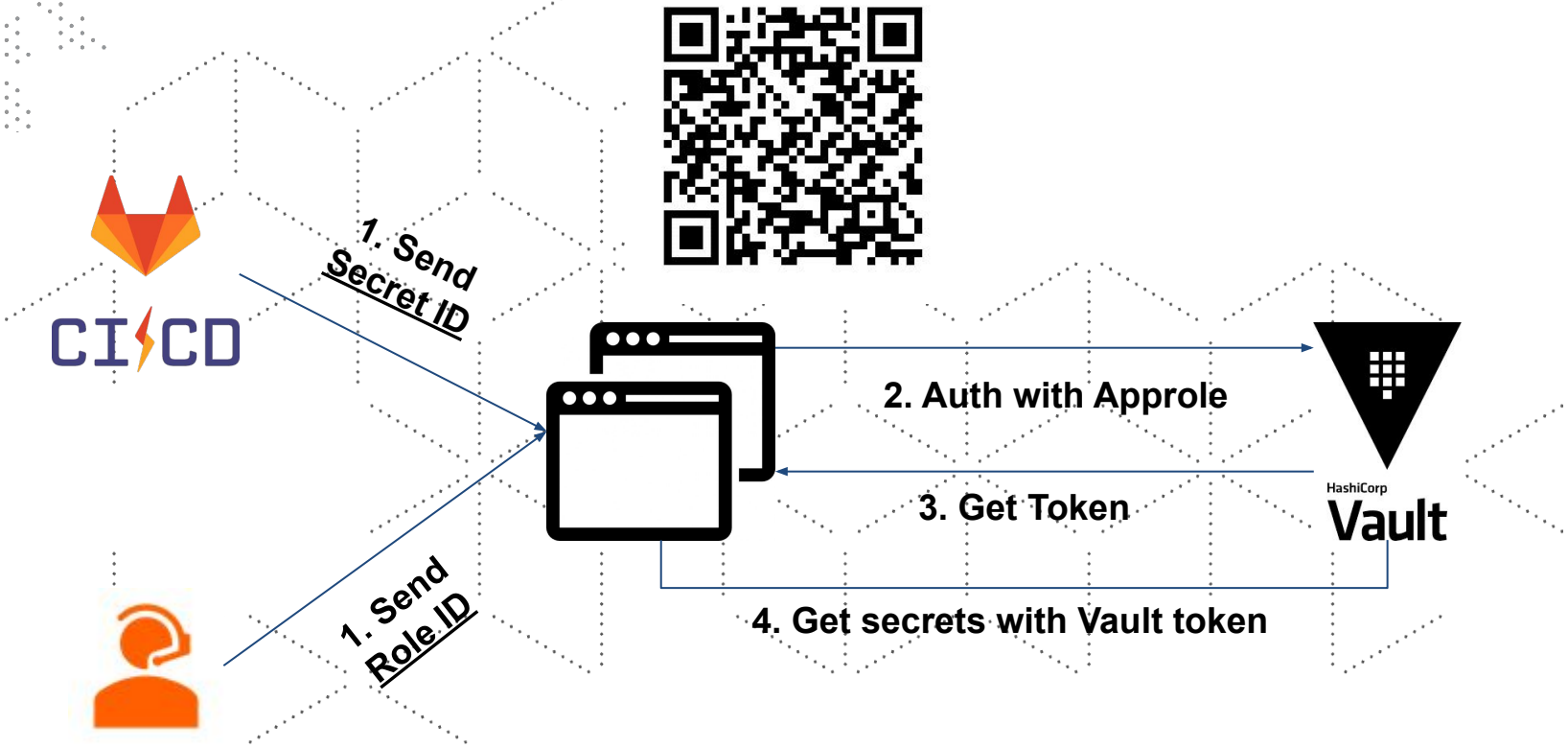
Steps to be a ninja



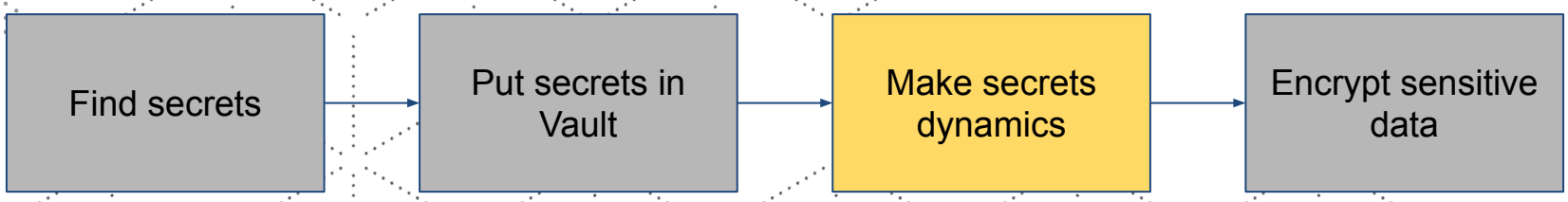
Approle


1. Create policy and role for apps
2. Get Role ID
3. Generate a new Secret ID
7. Return a token
6. Authenticate with Role ID and Secret ID
ADMIN
4. Deliver Role ID
5. Deliver Secret ID
APP

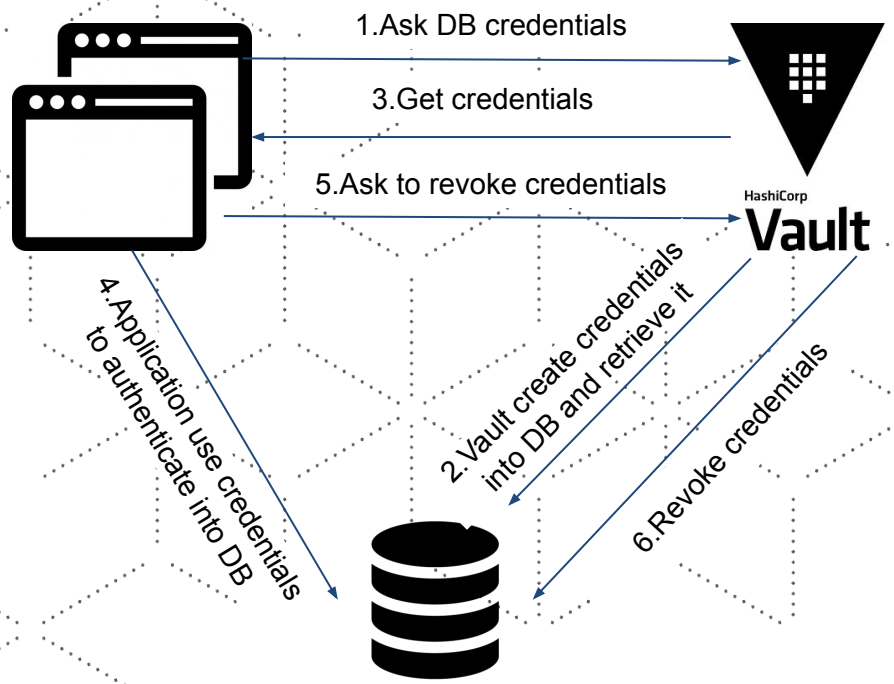
How is it working ?



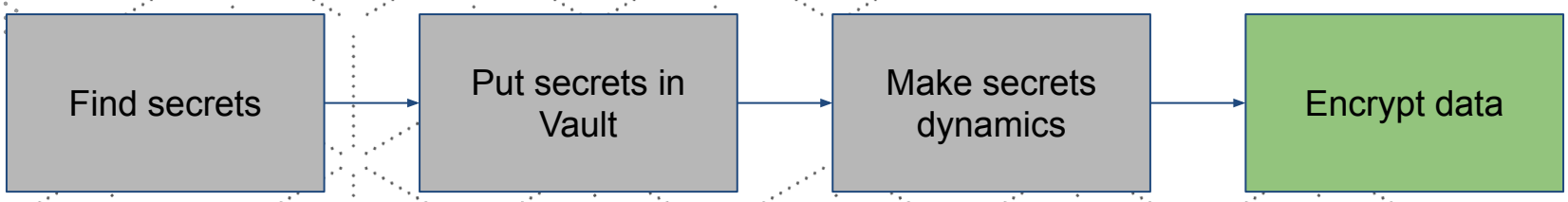
Steps to be a ninja



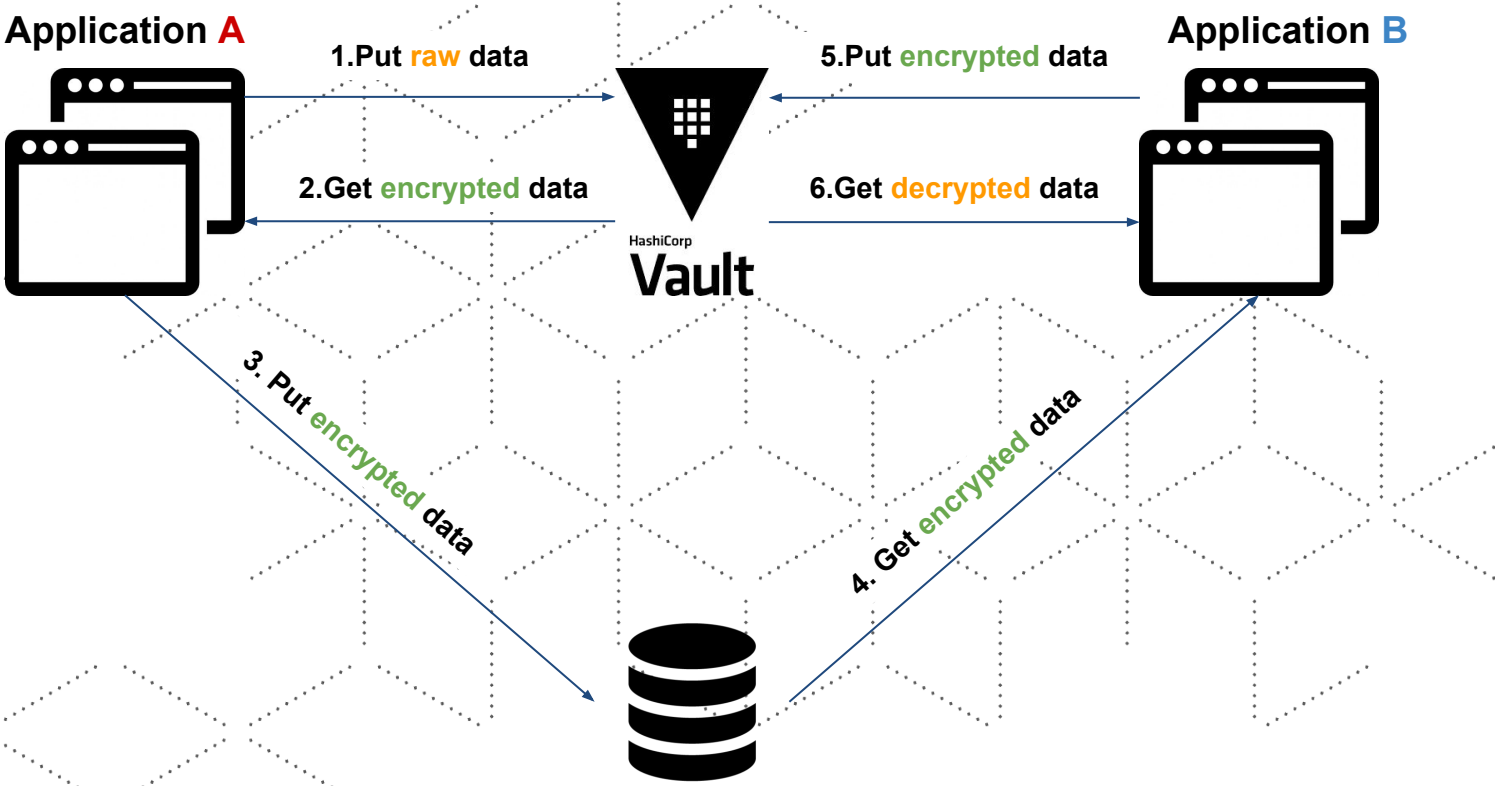
Secret as a Service



Steps to be a ninja



EaaS: Encryption as a Service



Demonstration

D2SI
by devoteam

To infinity... and beyond!

Consul service mesh

envconsul and / or consul-template

Vault Agent

Question ?

The last but not least

Trust nobody, not even yourself