Secrets Engines

Bryan Krausen
Sr. Solutions Architect
@btkrausen

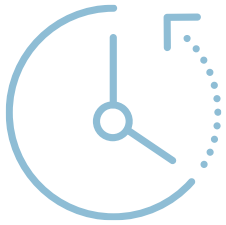
SKYLINES ACADEMY

Secrets Engines

- Difficulties of Managing Static Secrets
- Why You Should Use Dynamic Secrets
- Examples of Dynamic Secrets
- Introduction to Secrets Engines
- Secrets Engines Available in Vault
- How to Choose a Secrets Engine
- Secrets Engine Examples and Demos

Difficulties of Managing Static Secrets

SKYLINES ACADEMY



Expiration

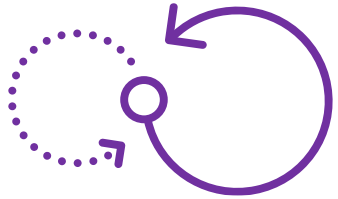
- Secrets never expire
- Required by legacy apps

Secrets Aren't Secret

- Secrets are often shared among team members
- No accountability

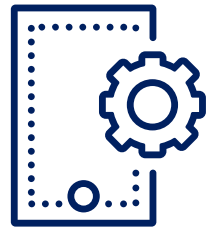
Validity

- Secrets are valid 24/7
- Frequently the target for penetrators



Rotation

- Secrets are rarely, if ever, rotated
- Manual process

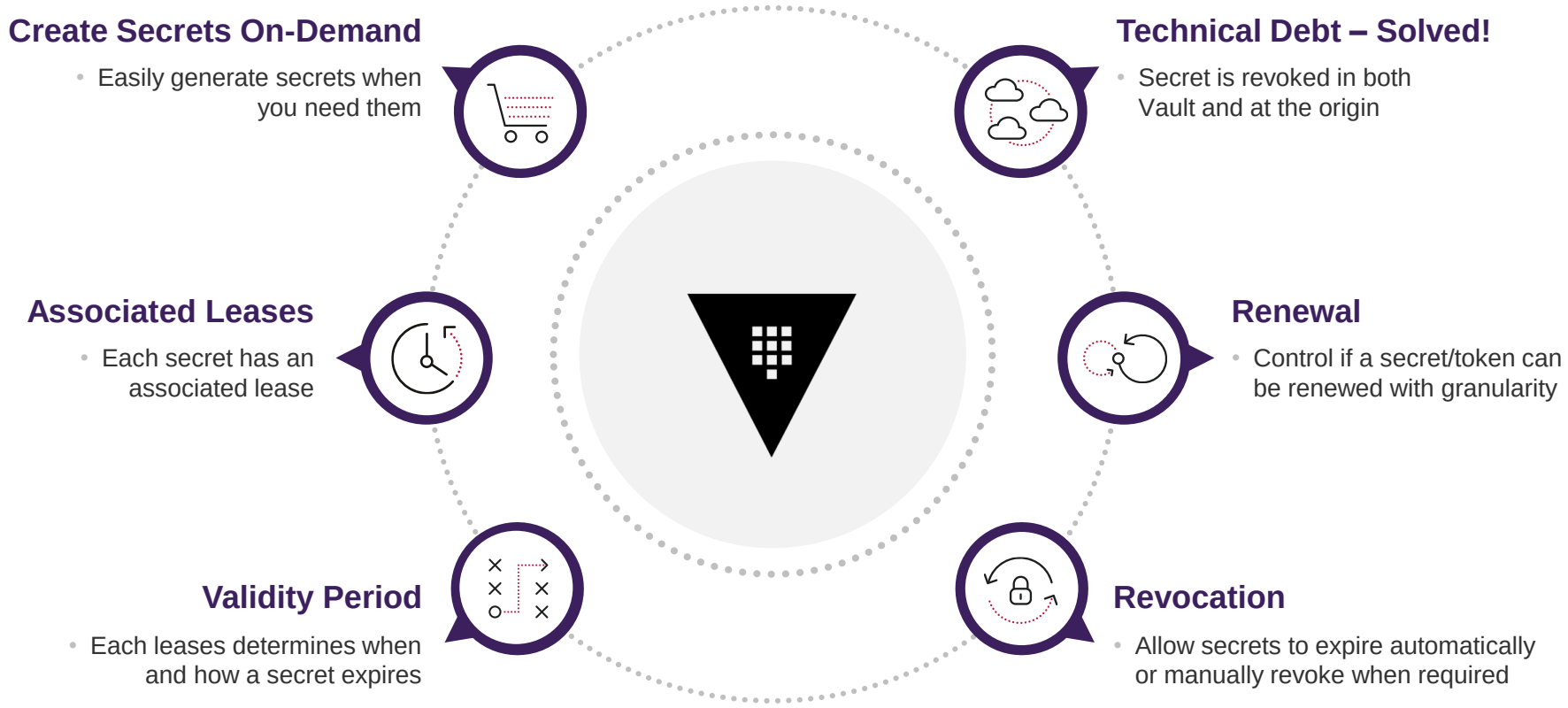


Long-Lived

- Secrets tend to live perpetually
- Result of technical debt, employee turnover, etc

Why You Should Use Dynamic Secrets

SKYLINES ACADEMY



Create Secrets On-Demand

- Easily generate secrets when you need them

Technical Debt – Solved!

- Secret is revoked in both Vault and at the origin

Associated Leases

- Each secret has an associated lease

Renewal

- Control if a secret/token can be renewed with granularity

Validity Period

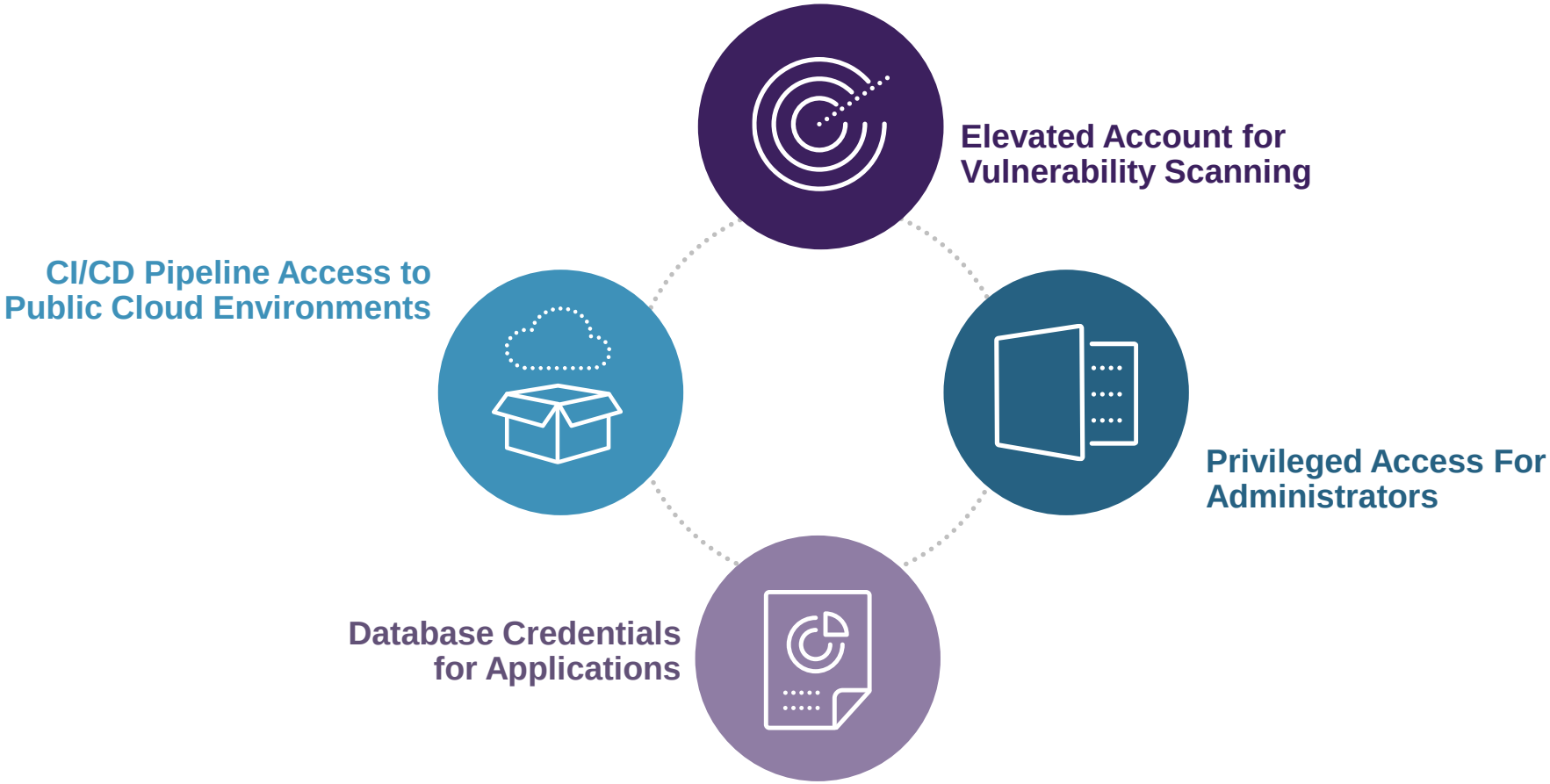
- Each leases determines when and how a secret expires

Revocation

- Allow secrets to expire automatically or manually revoke when required

Examples of Dynamic Secrets

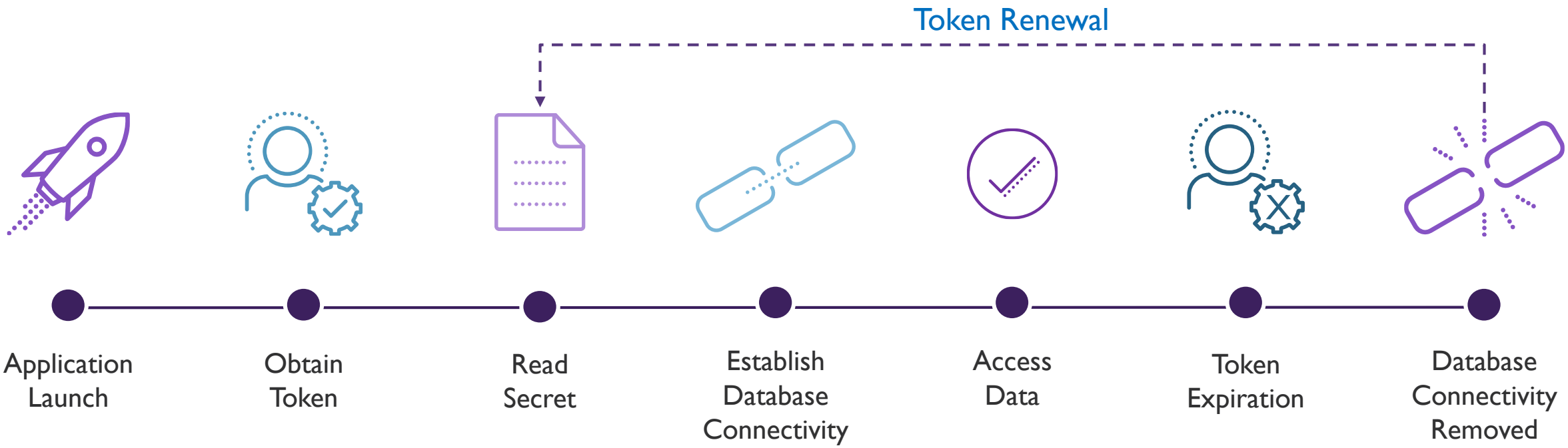
SKYLINES ACADEMY



Dynamic Secrets - Examples

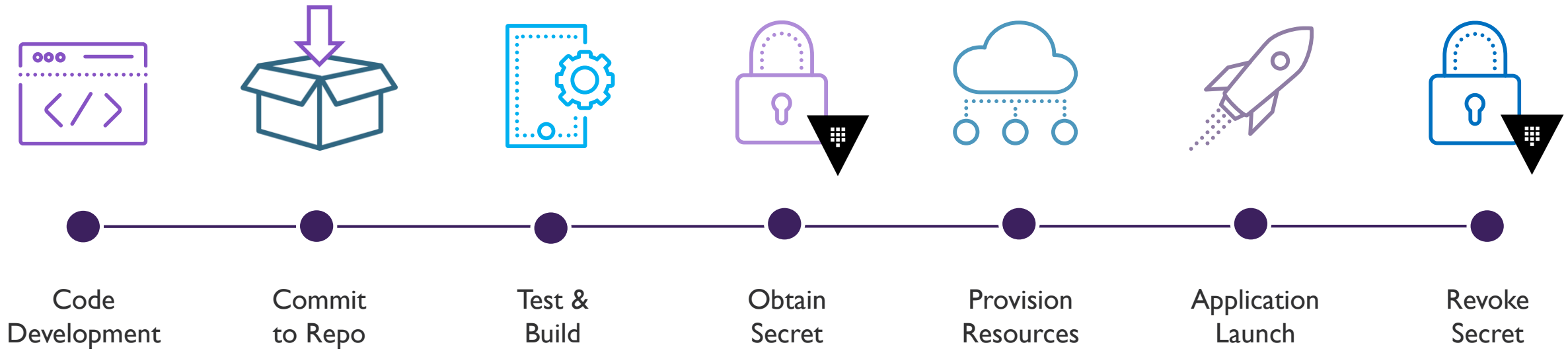
Example – Application Using Vault

SKYLINES ACADEMY



Example – Pipeline Using Vault

SKYLINES ACADEMY



Intro to Secrets Engines

SKYLINES
ACADEMY

Intro to Secrets Engines

SKYLINES ACADEMY

- Secrets engines are THE reason you deploy Vault
- Without secrets engines, there's really no point in using Vault

- Everything else up until this point can be considered as supporting components to secrets engine.

Intro to Secrets Engines

SKYLINES ACADEMY

- Secrets Engines can store, generate, or encrypt data
- Many secrets engines can be enabled and used as needed

- Secret engines are enabled and isolated at a "path"

```
$ vault secrets enable aws
```

- All interactions are done directly with the "path" itself

```
$ vault read aws/creds/aws_role
```

Secrets Engines in Vault

SKYLINES ACADEMY

- Active Directory
- AliCloud
- AWS
- Azure
- Consul
- Cubbyhole
- Databases
- Google Cloud
- Google KMS
- Identity
- KMIP
- Key/Value
- Nomad
- PKI (certs)
- RabbitMQ
- SSH
- TOTP
- Transit

Secrets Engines - Databases

SKYLINES ACADEMY

- Cassandra
- Elasticsearch
- Influxdb
- HanaDB
- MSSQL
- MySQL/MariaDB
- PostgreSQL
- Oracle
- Custom

Secrets Engines

SKYLINES ACADEMY

Amazon Web Services
Microsoft Azure
Google Cloud Platform
Google Cloud KMS
Alibaba Cloud

Apache Cassandra
InfluxDB
MongoDB
Microsoft SQL
MySQL/MariaDB
PostgreSQL
Oracle
SAP HANA

Active Directory
Consul
Cubbyhole
Key/Value
Identity
RabbitMQ
Nomad
SSH
TOTP

Transit
PKI

How to Choose a Secrets Engine

SKYLINES ACADEMY

Store

- K/V

Generate

- AWS
- Database
- Active Directory
- TOTP
- PKI

Encrypt

- Transit

Secrets Engines - Examples

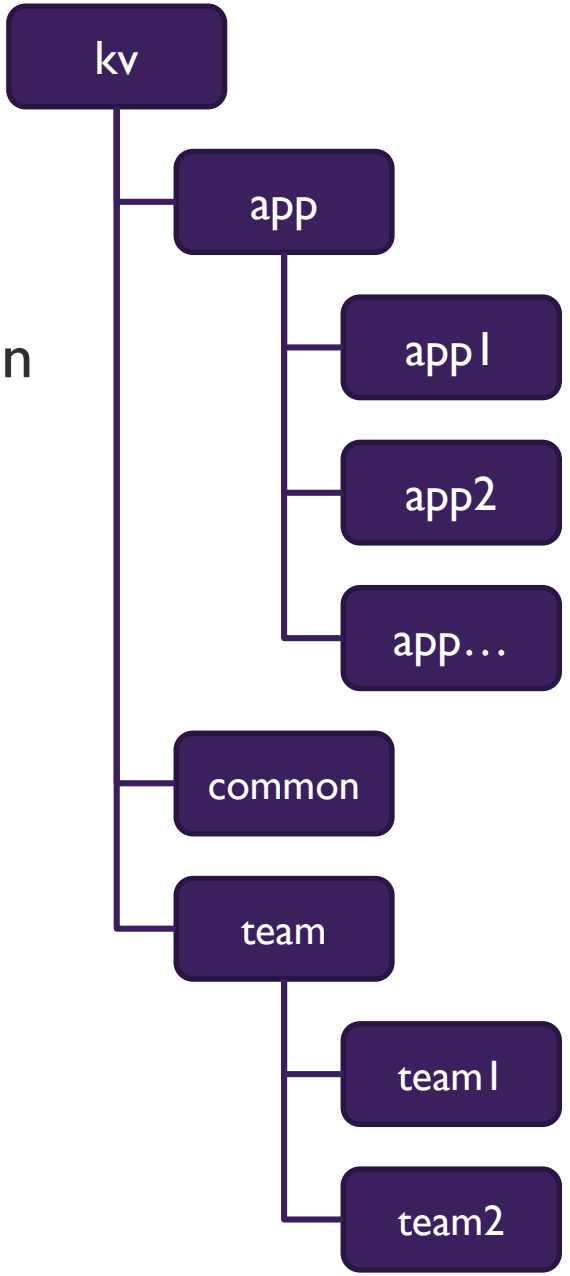
Key/Value (KV) Secrets Engine

SKYLINES ACADEMY

- Allows you to store any information you'd like as a key & value
  - For example – secrets/webapp1/creds
    - user: skylines
    - password:skylines123!
- The most frequently used secrets engine in Vault
- Two versions available, named v1 and v2
  - KV v1 is the traditional version with standard features
  - KV v2 supports versioning

KV Structure

- Create a foundational structure
- Use parameters to simplify policies for administration
- Group by applications and teams
- Create additional mounts, if easier to manage
- Every KV structure will be different, although you should standardize between environments, where possible



DEMO

KV Secrets Engine

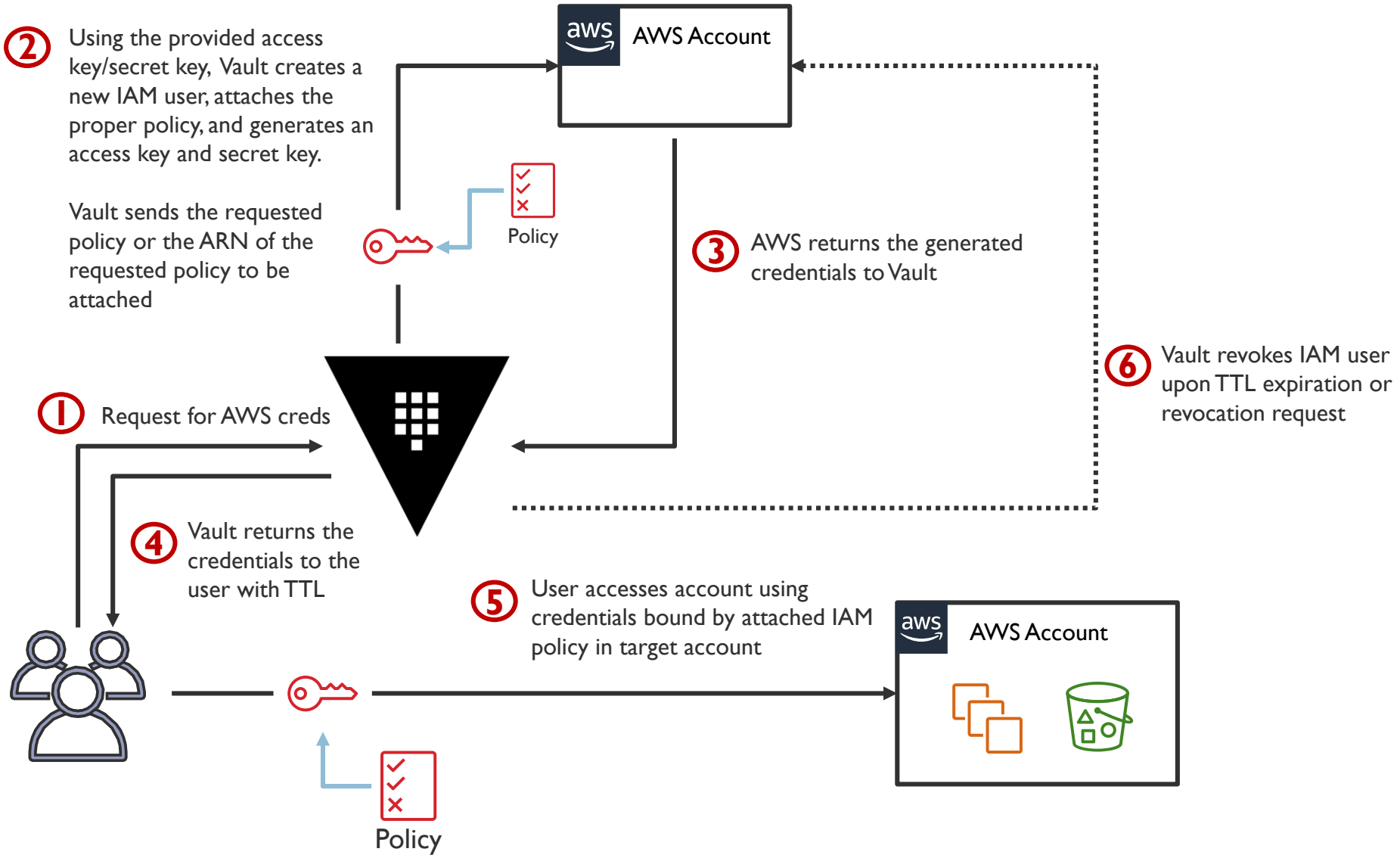
AWS Secrets Engine

SKYLINES ACADEMY

- Dynamically generates AWS credentials
- Credentials still bound to a policy to permit/restrict actions
- Simply to configure for basic usage
  - Can be trickier when using for multiple accounts
- Three types of ways to generate creds:
  - iam_user – generates an IAM user with access and secret key
  - assumed_role – uses sts:AssumeRole to generate creds
  - federation_token – sts:GetFederationToken

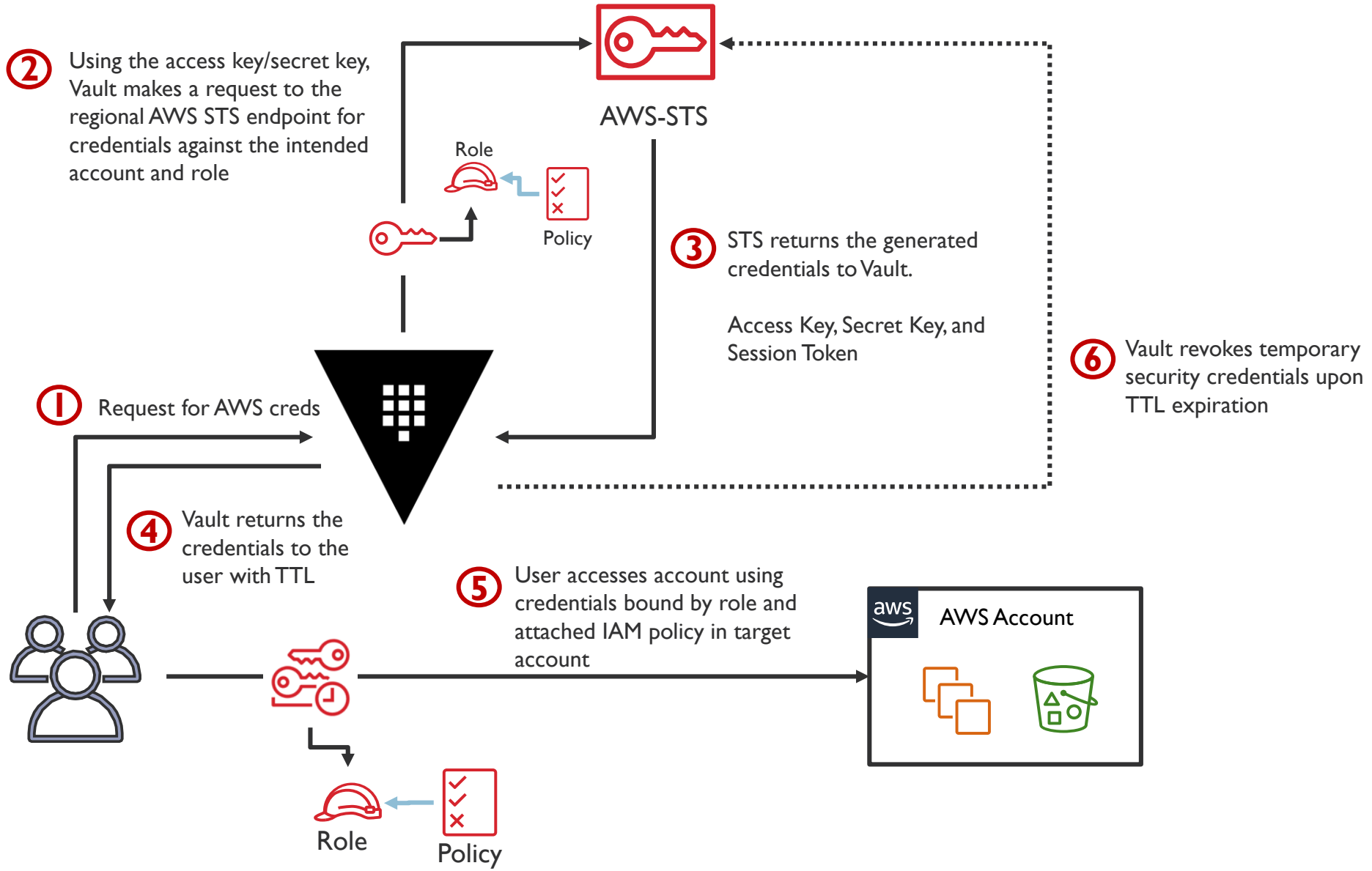
IAM User

SKYLINES ACADEMY



Assume Role

SKYLINES ACADEMY



DEMO

AWS Secrets Engine

Secrets Engines

- Difficulties of Managing Static Secrets
- Why You Should Use Dynamic Secrets
- Examples of Dynamic Secrets
- Introduction to Secrets Engines
- Secrets Engines Available in Vault
- How to Choose a Secrets Engine
- Secrets Engine Examples and Demos

SECTION RECAP

SKYLINES ACADEMY

SKYLINES

ACADEMY