Join us for KubeCon + CloudNativeCon Virtual

Event dates: **August 17-20, 2020**

Schedule: **[Now available!]**

Register now!

CYBERARK®

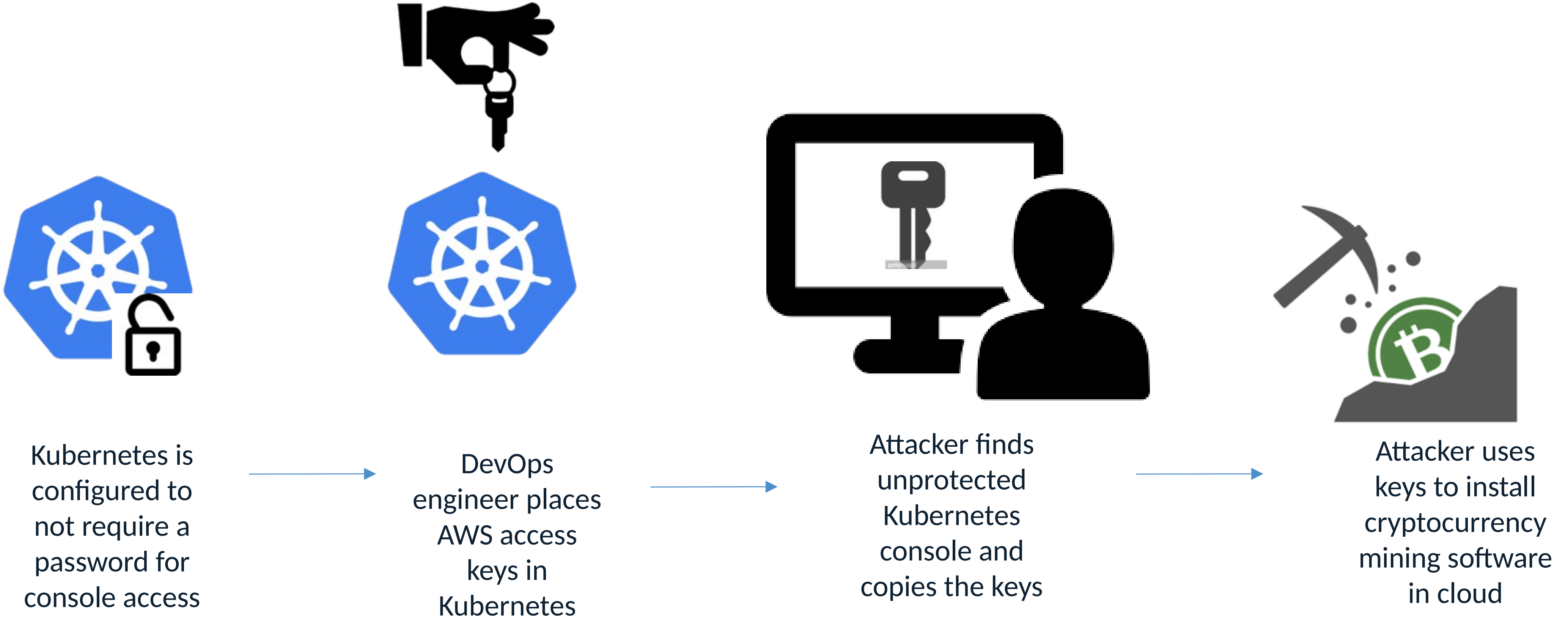
KUBERNETES SECRETS MANAGEMENT

Build Secure Apps Faster Without Secrets

ATTACKERS TARGET APPLICATION SECRETS

Tesla Cloud Account Data Breach

Attackers used credentials stored in Kubernetes to hijack cloud resources to mine cryptocurrency



Kubernetes is configured to not require a password for console access

DevOps engineer places AWS access keys in Kubernetes

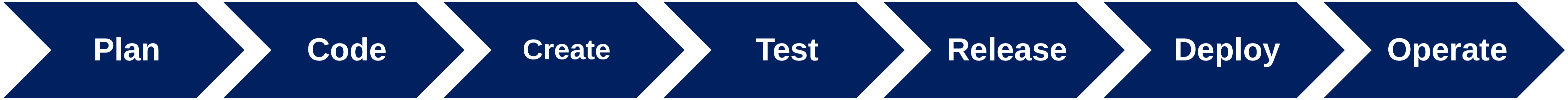
Attacker finds unprotected Kubernetes console and copies the keys

Attacker uses keys to install cryptocurrency mining software in cloud

EVERYBODY WANTS A SECURE DEVOPS FLOW, BUT…

"I hate it when we fight."

SHIFTING SECURITY LEFT INTO DEVELOPMENT WORKFLOWS



Plan

Code

Create

Test

Release

Deploy

Operate

Enable Developer/DevOps

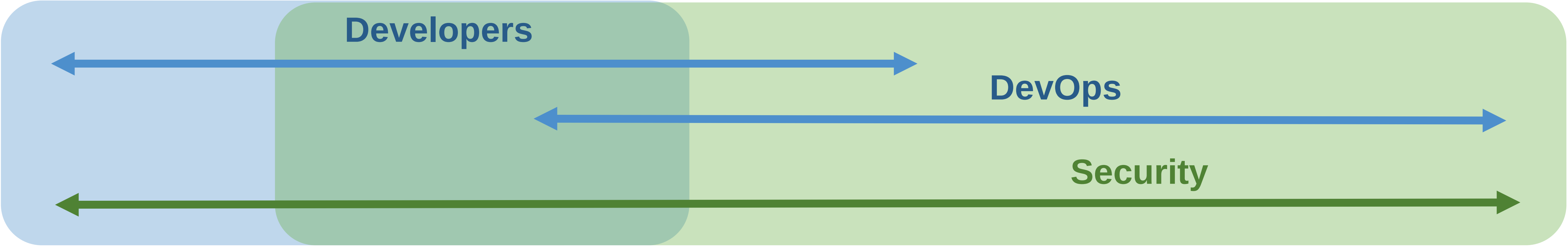
- Easy to use (consume secrets)
- Prebuilt integrations
- Conjur Open Source and Secretless Broker

Free developers from security burden

- Compliance, audit requests, human creds
- Security budget

Empower security team

- Highlight the app & tool risk
- Leverage single platform – human/non-human solution serves all
- Security focus
- Manage security budget



Developers

DevOps

Security

BEST PRACTICES FOR SECURING SECRETS

Removal of Hard-Coded Credentials	Establish Identity to Applications	Credential Rotation
Limit Secret Leaks & Reduce Attack Surface	Create Auditable Identity for Apps	Regularly Perform Secrets Rotation
Enables Compliance with Audit & Best Practices	Authorized Access that is	Limit Updates to Files, Code or DBs when Secrets Rotated
Remove Security Islands	Enforce Strong Authn for Apps, Remove Secrets Zero	Limit Application Downtime Required to Rotate Secrets

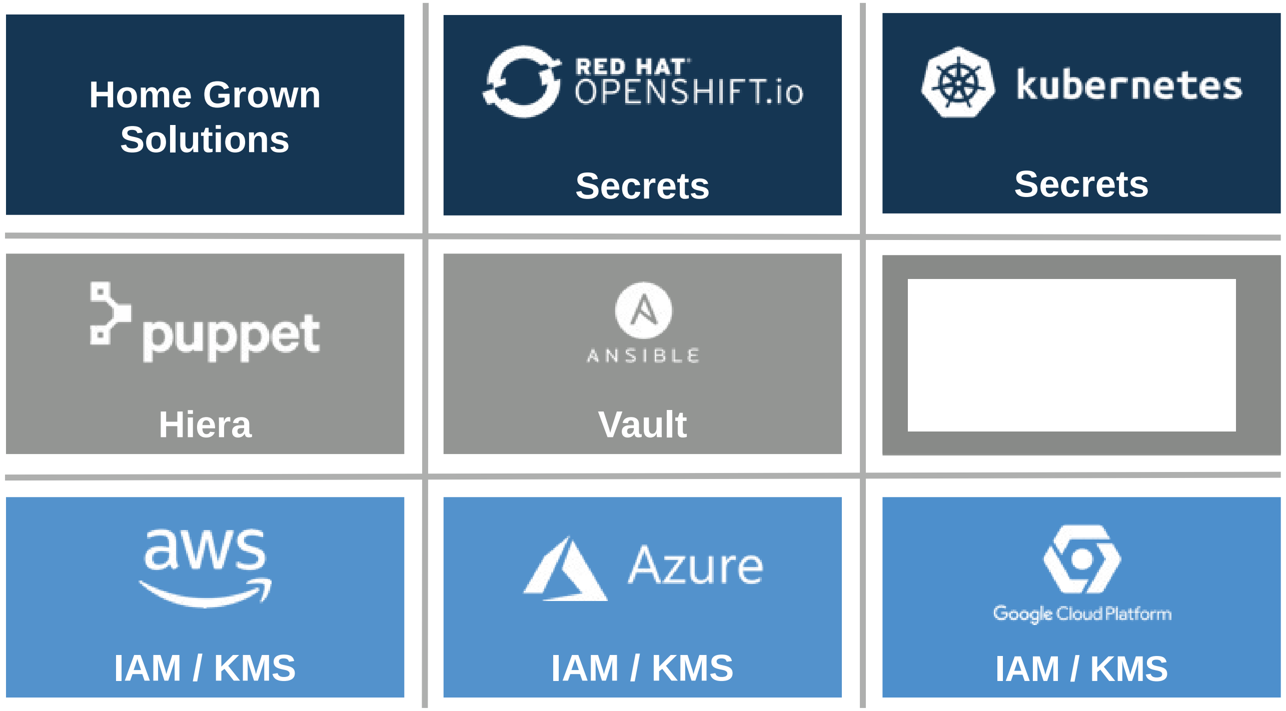
THE PROBLEMS WITH SECURITY ISLANDS

There are many ways to vault secrets,

But:

- Developers must learn multiple solutions
- Hard to establish & share best-practices
- Short-cuts often taken
- SoD not enforced
- GRC reporting is impossible

Islands of Security



Home Grown Solutions	RED HAT OPENSHIFT.io Secrets	kubernetes Secrets
puppet Hiera	ANSIBLE Vault	
aws IAM / KMS	Azure IAM / KMS	Google Cloud Platform IAM / KMS

IF IT CAN BE IDENTIFIED, ITS ACCESS CAN BE MANAGED

- Build on a chain of trust
  - Authenticate all requests
  - Authorize w/ least amount of privilege
  - Audit everything
  - ...and do it with code!

Human Identity

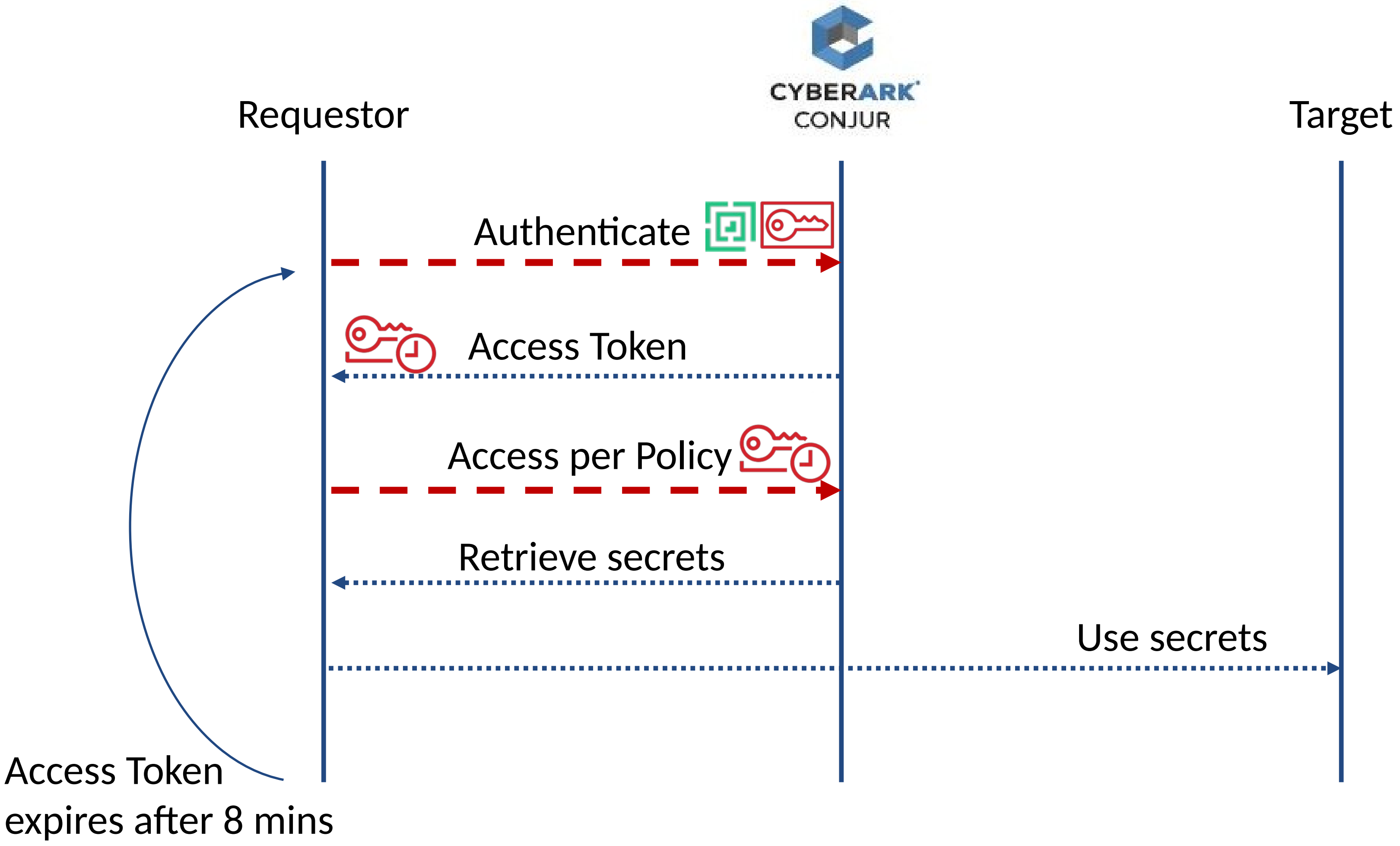
Machine Identity

- The Secret-Zero Problem…
  - Humans use their built-in vault for passwords or, failing that, answers to security questions.
  - Non-humans need a way to bootstrap identity that doesn't put credentials at risk
  - But how to manage that initial secret required by apps to bootstrap identity?

WAYS TO ESTABLISH & AUTHENTICATE IDENTITY

	Use-Case	Means	Strengths	Weaknesses
Credential Based	**Human identity**	Passport, Password	• Very familiar • Humans have built-in vaults	• Social engineering • Insecure persistent storage
	Pre-Configured Identity	API Key	Analogous to human uname/pwd model	• Key distribution is subject to compromise • Requestor can’t initiate
	Bootstrapped Identity	Token-based	• Can provide extra control factors, e.g. time, CIDR, one-time use, etc.	• Secret to get a secret • Stateful - requires active entropy mgmt
Attribute Based	**Human Identity**	Biometrics	• Hard to spoof • Convenient	• Context dependent
	Pre-Configured Identity	Various Factors	• Multi-factor (selectable) • OS user, path, MD5 hash, IP/Hostname	• No trusted 3rd party • Requires authn agent running local to applications • Not scalable to container use-cases
	Bootstrapped Identity	Trusted 3rd Party	• Ideal for container orchestration	• Platform dependencies • Hard to implement for legacy technologies

SECRETS ACCESS WORKFLOW



K8S ATTRIBUTE AUTHENTICATION IN

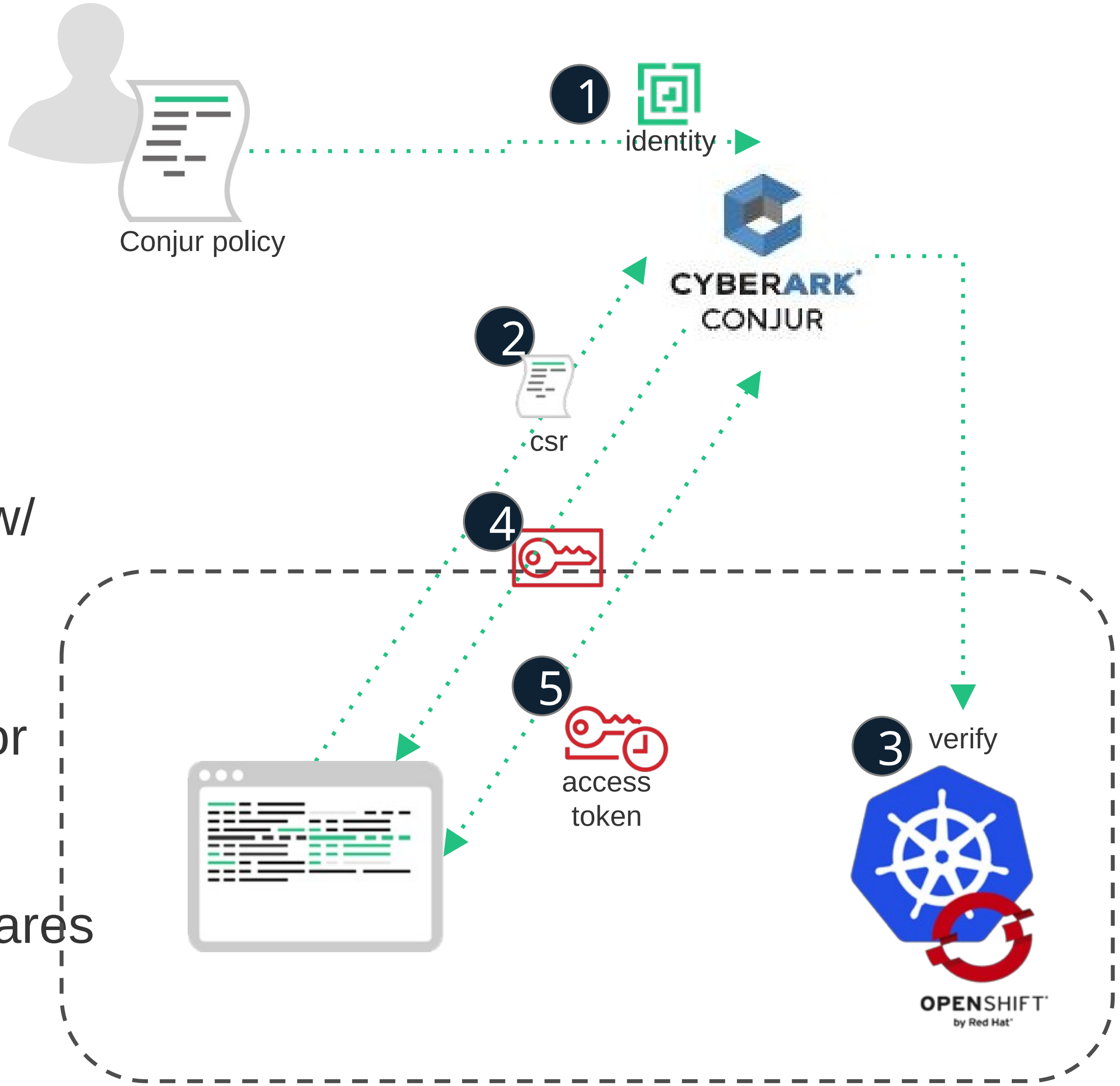
1) Admin whitelists app identity with Conjur

   Three options for identity granularity:

   - Identity = Cluster/Namespace
   - Identity = Cluster/Namespace/Service Account

2) Authenticator client in app pod submits CSR w/ platform attributes to Conjur

3) Conjur verifies attributes w/ platform service
4) Conjur issues cert & key creds to authenticator client in app pod
5) Authenticator client in app pod uses creds to authenticate, get Conjur access token and shares via shared memory volume.

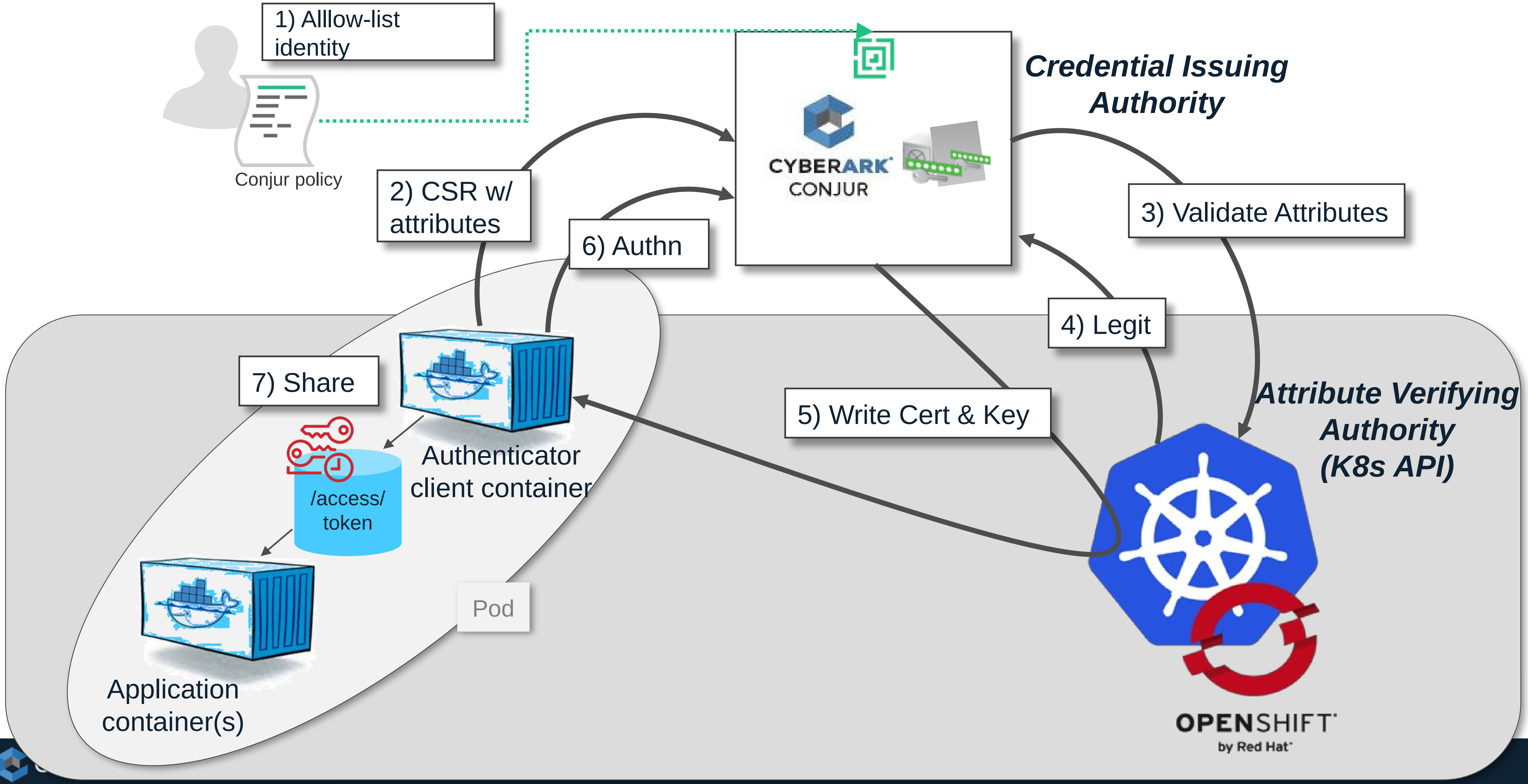


AUTHENTICATE WORKLOADS, NOT INFRASTRUCTURE

Secure Production Identity Framework for Everyone

Inspired by the production infrastructure of Google and others, SPIFFE is a set of open-source standards for securely identifying software systems in dynamic and heterogeneous environments.

IDENTITY VERIFIED USING K8S PLATFORM ATTRIBUTES



CONJUR DEMO USE-CASES

- **Lab 1: {REST-API}**
  - Authenticator runs as a Sidecar
  - App pulls DB creds with REST API
  - App connects to DB

- **Lab 2: Secrets Injection w/ Summon**
  - Authenticator runs as an Init container
  - Summon pulls DB creds & calls app w/ creds in env vars
  - App connects to DB

- **Lab 3: K8s Secrets**
  - Authenticator runs as an Init Container
  - K8s secret manifest names DB cred names
  - Authenticator retrieves DB creds & dynamically patches K8s secret w/ DB cred values
  - App connects to DB

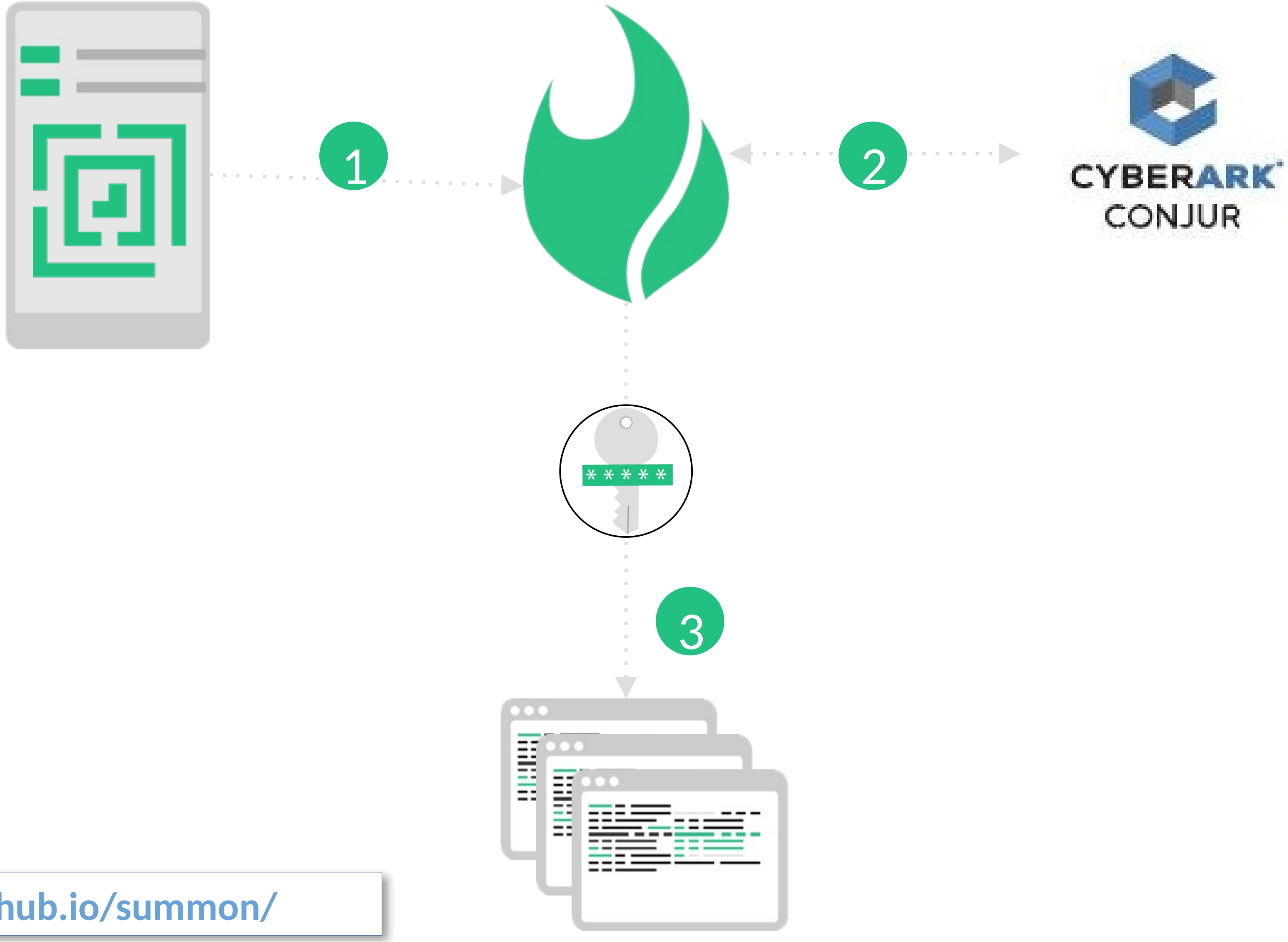
- **Lab 4: Secretless Broker**
  - Authenticator runs as a Sidecar Container listening on DB port
  - App attempts to connect to DB on local port
  - Authenticator retrieves DB creds, connects to DB, proxies connection for app
  - App connects to DB

Summon for secrets injection

1 Summon invoked with authenticated identity

2 Summon fetches secrets using identity

3 Processes launched with secrets in environment



Learn more at: https://cyberark.github.io/summon/

THE SECRETS LIFECYCLE TODAY

Secrets Storage

Secrets Delivery

Applications

BRINK'S
A DIVISION OF THE PITTSTON COMPANY
SECURITY SINCE 1859

INTRODUCING “SECRETLESS”

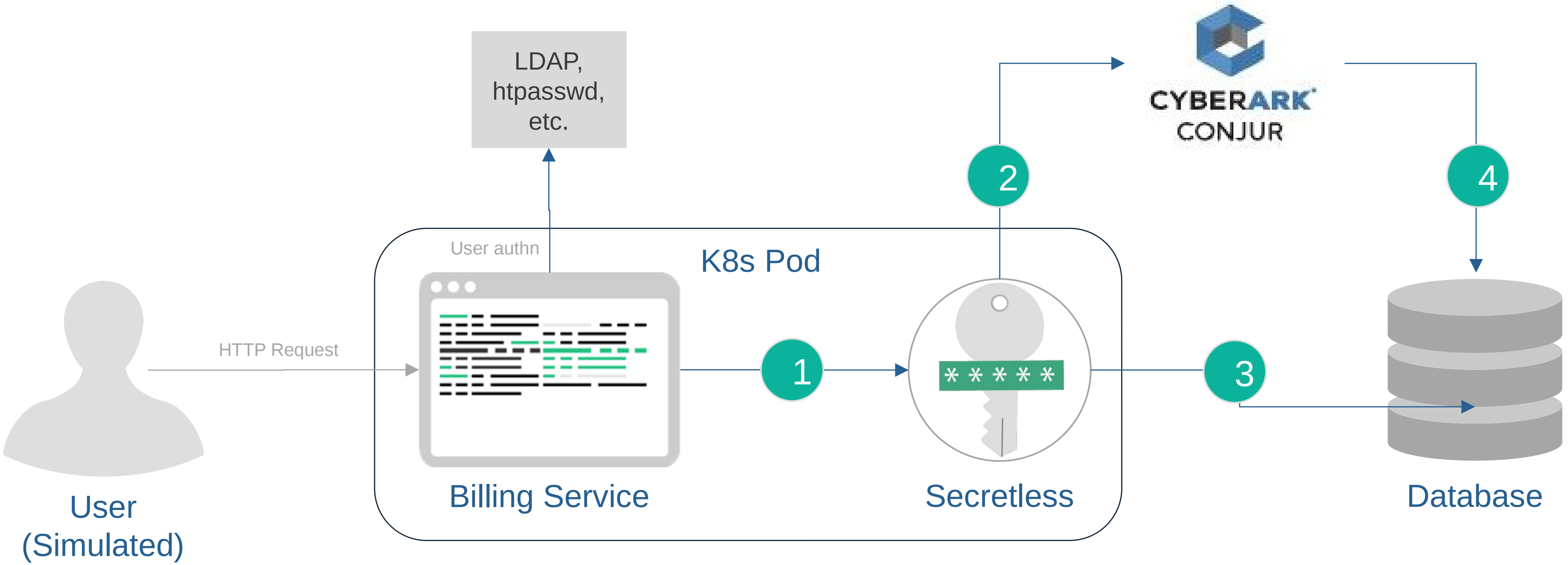
Establishes proxied connections to resources w/o direct access to secrets.

- Frees developers and applications from responsibility of managing secrets.
- Reduces the threat surface of secrets
- Handles rotation transparently
- Does not change how clients connect to services
- Allows use of standard libraries and tools.

Uses an extensible driver model to connect to backend resources.

- For example:
  - HTTP
  - SSH (MITM and ssh-agent approaches)
  - SQL and NoSQL Databases
  - New drivers in development, inquire within to join the effort.

“SECRETLESS” CONCEPT: APPS CAN’T LEAK SECRETS



1 Service connects to Secretless proxy

2 Secretless proxy requests database credentials to remote database

3 Secretless establishes a connection to the remote database and transparently brokers the connection

4 Conjur seamlessly rotates database credentials used by Secretless

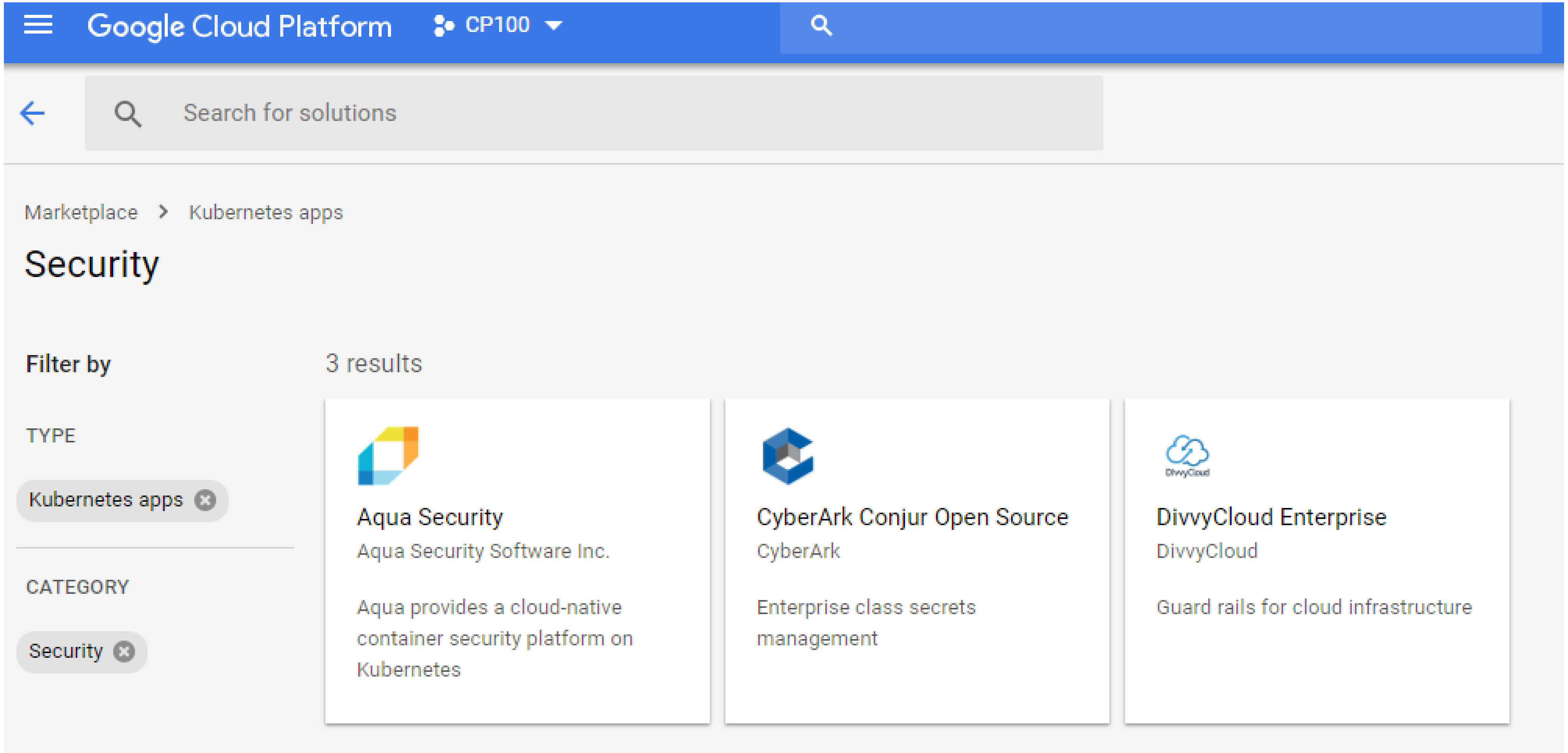
Stolen secrets? Inconceivable!

BENEFITS

- ✓ Simple, context free, secure method for retrieving credentials in containers
- ✓ End-to-end encryption of secrets through mutual TLS (Transport Layer Security) using SPIFFE-compliant resource identifiers.
- ✓ Robust authentication and authorization incorporating Conjur policy, signed certificates, and an internal Kubernetes APIs.
- ✓ Conjur running inside Kubernetes
- ✓ SoD between applications
  - ✓ SoD also between the Kubernetes security operator and the development teams using Conjur policy
- ✓ Credentials are not exposed to any 3rd party, reside only in memory
- ✓ Full central audit trail

KUBERNETES – CONJUR INTEGRATION IN GOOGLE MARKETPLACE

DEPLOY CONJUR INTEGRATION IN KUBERNETES IN JUST A FEW CLICKS!



Marketplace > Kubernetes apps

Security

Filter by

TYPE

Kubernetes apps ☒

CATEGORY

Security ☒

3 results

Aqua Security
Aqua Security Software Inc.
Aqua provides a cloud-native container security platform on Kubernetes

CyberArk Conjur Open Source
CyberArk
Enterprise class secrets management

DivvyCloud Enterprise
DivvyCloud
Guard rails for cloud infrastructure

CONJUR OPEN SOURCE AND THE CYBERARK OPEN SOURCE COMMUNITY

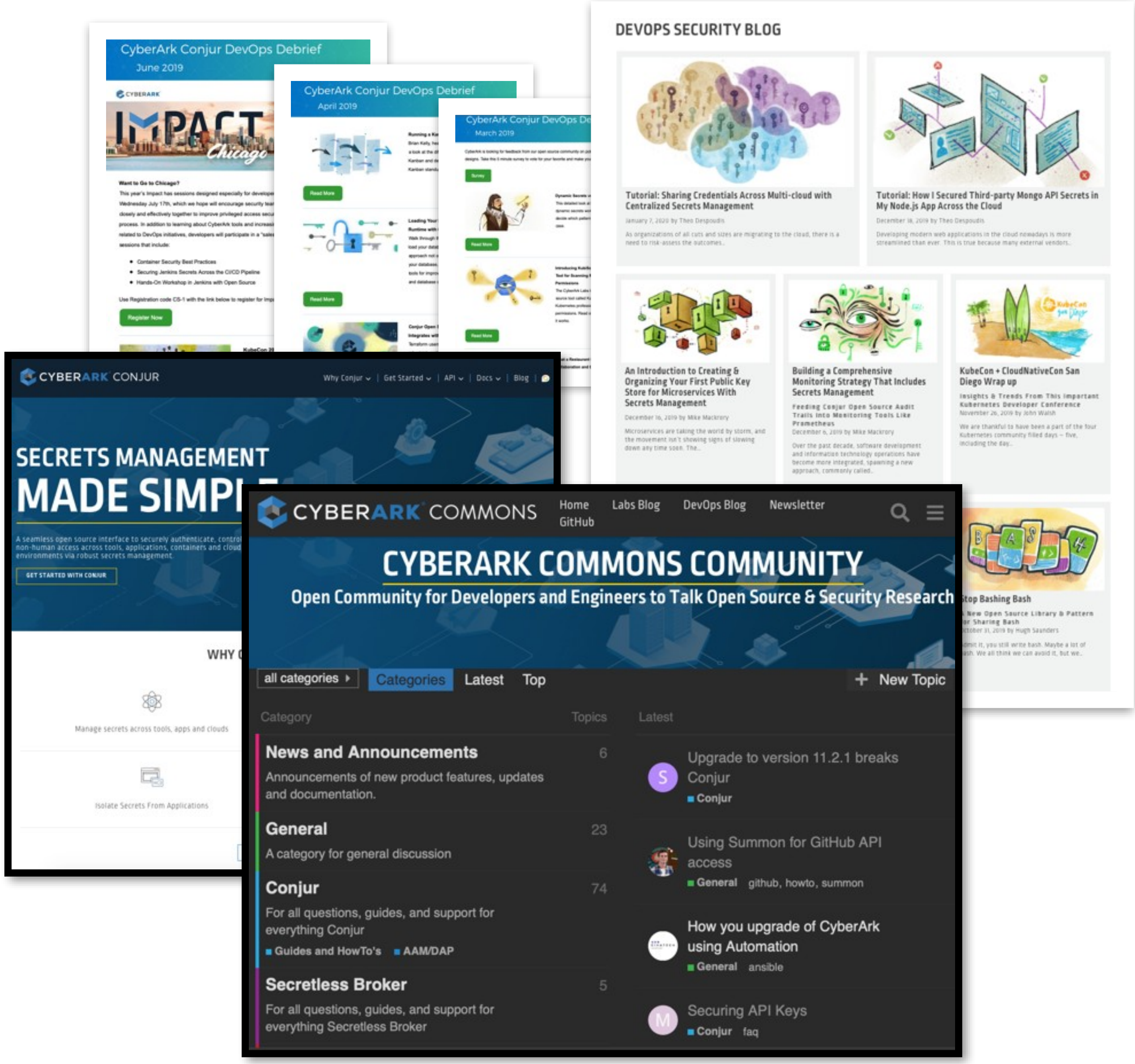
CyberArk Commons OSS Community:

- Conjur.org
  - APIs, documents, tutorials, code
  - New technical content each month: blogs, newsletter
  - Streamlined user experience to get started and get hands on
- Discuss.CyberArkCommons.org
  - Discussions and community support for open source

- Hands-on Workshops, developer community events and forums

- Secretless Broker: Conjur.org/api/secretless-broker

- Summon: CyberArk.GitHub.io/Summon



CyberArk Conjur DevOps Debrief
June 2019

IMPACT Chicago

Want to Go to Chicago?

Register Now

CyberArk Conjur DevOps Debrief
April 2019

Read More

CyberArk Conjur DevOps Debrief
March 2019

DEVOPS SECURITY BLOG

Tutorial: Sharing Credentials Across Multi-cloud with Centralized Secrets Management
January 7, 2020 by Theo Despoudis
As organizations of all cuts and sizes are migrating to the cloud, there is a need to risk-assess the outcomes…

Tutorial: How I Secured Third-party Mongo API Secrets in My Node.js App Across the Cloud
December 18, 2019 by Theo Despoudis
Developing modern web applications in the cloud nowadays is more streamlined than ever. This is true because many external vendors…

An Introduction to Creating & Organizing Your First Public Key Store for Microservices With Secrets Management
December 16, 2019 by Mike Mackrory
Microservices are taking the world by storm, and the movement isn't showing signs of slowing down any time soon. The…

Building a Comprehensive Monitoring Strategy That Includes Secrets Management
Feeding Conjur Open Source Audit Trails into Monitoring Tools Like Prometheus
December 6, 2019 by Mike Mackrory
Over the past decade, software development and information technology operations have become more integrated, spawning a new approach, commonly called…

KubeCon + CloudNativeCon San Diego Wrap up
Insights & Trends From This Important Kubernetes Developer Conference
November 26, 2019 by John Walsh
We are thankful to have been a part of the four Kubernetes community filled days – five, including the day…

…top Bashing Bash

CYBERARK CONJUR

Why Conjur | Get Started | API | Docs | Blog

SECRETS MANAGEMENT MADE SIMPLE

A seamless open source interface to securely authenticate, control non-human access across tools, applications, containers and cloud environments via robust secrets management

GET STARTED WITH CONJUR

Manage secrets across tools, apps and clouds

Isolate Secrets From Applications

CYBERARK COMMONS

Home Labs Blog DevOps Blog Newsletter GitHub

CYBERARK COMMONS COMMUNITY

Open Community for Developers and Engineers to Talk Open Source & Security Research

all categories ▸ Categories Latest Top + New Topic

Category	Topics	Latest
News and Announcements Announcements of new product features, updates and documentation.	6	Upgrade to version 11.2.1 breaks Conjur Conjur
General A category for general discussion	23	Using Summon for GitHub API access General github, howto, summon
Conjur For all questions, guides, and support for everything Conjur Guides and HowTo's AAM/DAP	74	How you upgrade of CyberArk using Automation General ansible
Secretless Broker For all questions, guides, and support for everything Secretless Broker	5	Securing API Keys Conjur faq

CYBERARK

THANK YOU

CONJUR.ORG
DISCUSS.CYBERARKCOMMONS.ORG