



# PRIVILEGED SECURITY FOR NETOPS

Quincy Cheng – APJ DevOps Manager, CyberArk

# DEVOPS, NETOPS, SECOPS, DEVSECOPS...

- Net – Network
- Dev – Development
- Ops – Operations
- Sec – Security

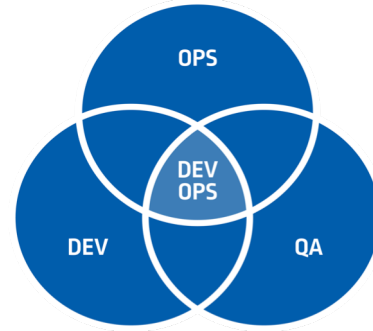


# WHY?



Everything is Code

NetOps: IAS  
Infrastructure as Code



Collaboration and  
Sync



Automation Continues  
Everything

It's all about **velocity** and delivering in  
a mode of **continuous improvement**

# CODE DELIVERY = REVENUE GROWTH



Companies with faster code delivery were

**62%**

more likely to see YoY revenue growth of 25% or more

Source: EMA, "DevOps/Continuous Delivery Tooling: Launchpad for the Digital Enterprise," 2017.



# 3 TYPICAL USE CASES

I manage projects, e.g.  
new deployments



**Jenkins**

***Project  
Manager***

I preform system  
operations, e.g. failover



ANSIBLE

***System  
Admin***

I manage infrastructure  
platforms, e.g. config &  
security baseline



**RED HAT**  
**OPENSIFT**  
Container Platform

***Infra-  
structure***

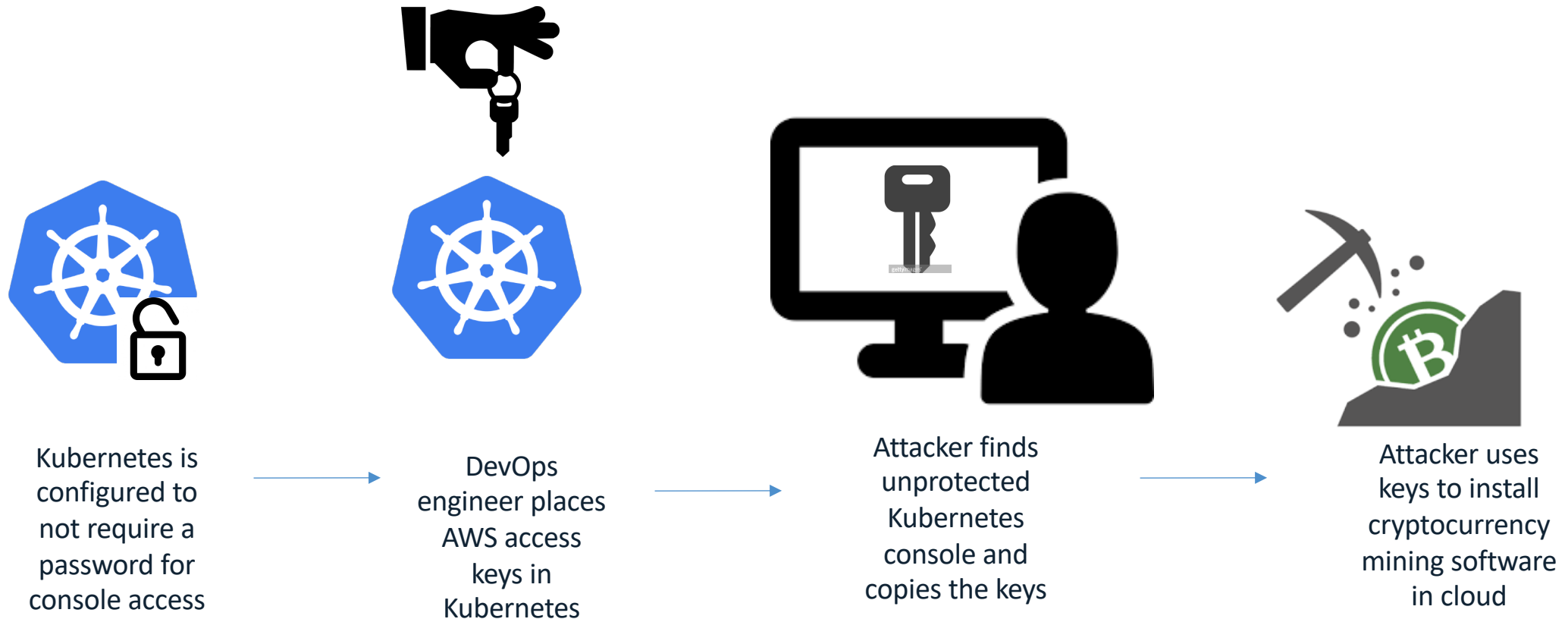
# REALITY



# ATTACKERS TARGET NON-HUMAN CREDENTIALS

## Tesla Cloud Account Data Breach

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



# ATTACK CAN BE SIMPLE

Search · aws\_access\_key

tweak aws access key for

Create new AWS secure a

Update AWS access keys

Delete aws-access-key.d


Quincy Cheng a...

← → ↻

GitHub, Inc. [US]

https://github.com/search?p=2&q=aws\_access\_key&type=Commits

🔍 ☆ 🔄 ⌵

 aws\_access\_key

/

Pull requests

Issues

Marketplace

Explore

🔔 + ▾ 🏠 ▾

Repositories61

Code102K

Commits6K

Issues1K

Topics

Wikis377

Users

[Advanced search](#) [Cheat sheet](#)

6,404 commit results

Sort: Best match ▾


Adjusting aws\_access\_key\_id and aws\_secret\_access\_key

Verified

📄

ff0cdb5

<>


 venezia committed to samsung-cnct/cluster-manager-api 26 days ago ✓

Prints out AWS profile and access key during client build

📄

1422018

<>


 niccottrell committed to niccottrell/mongo-metadata-s3 2 days ago

update aws access key

📄

4d83ccd

<>


 bouzuya committed to bouzuya/bouzuya.net on May 5 ✓

adds AWS Access Key info to README

📄

54b67fe

<>

 tomweston committed to axoe/gatekeeper 20 days ago

WIP - updated AWS access id and key

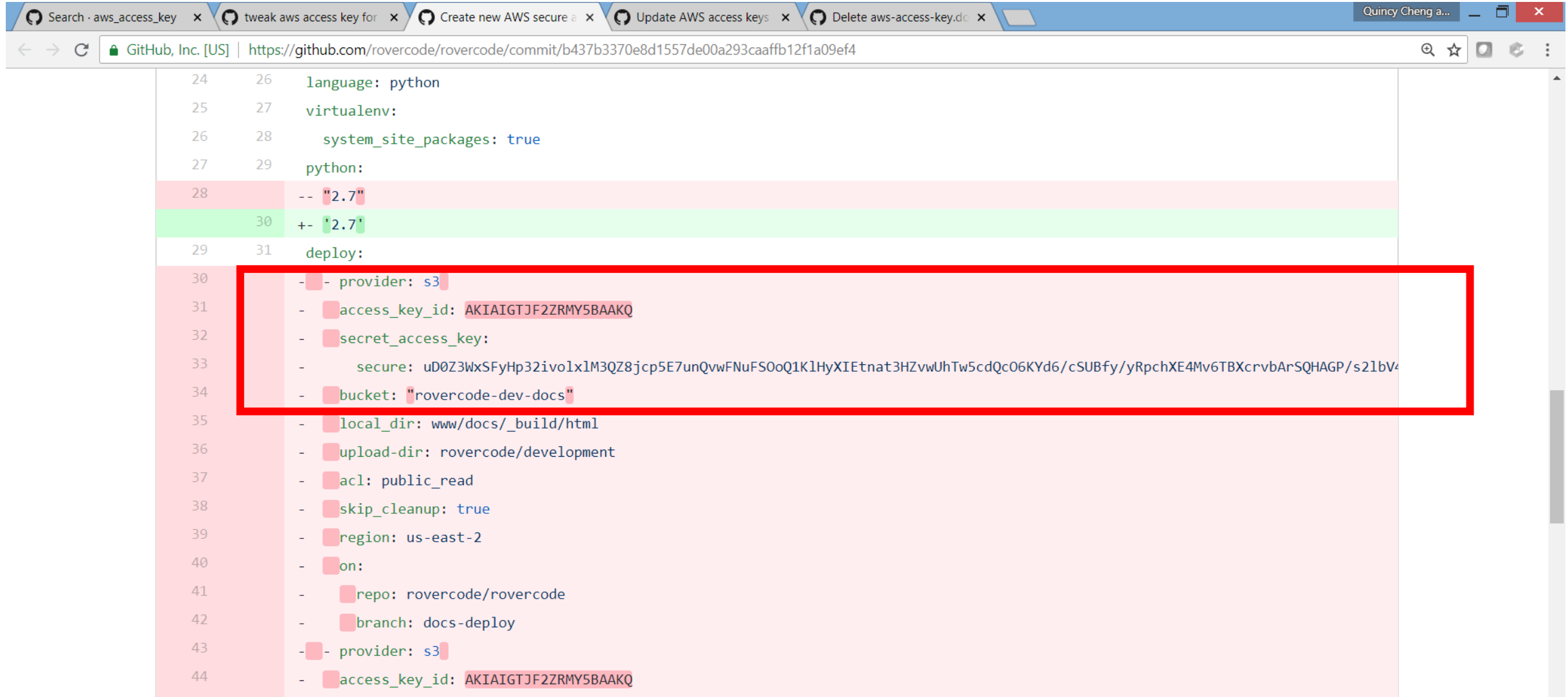
📄

a7da012

<>



# THE PROBLEM: EMBEDDED SECRETS












The screenshot shows a web browser displaying a GitHub commit page. The browser's address bar shows the URL: `https://github.com/rovercode/rovercode/commit/b437b3370e8d1557de00a293caaffb12f1a09ef4`. The page content shows a diff of a configuration file. The diff highlights changes to the `python` and `deploy` sections. A red rectangular box is drawn around the `deploy` section, which contains several lines of configuration, including AWS credentials and a long secure string. The configuration is as follows:

```
24 26 language: python
25 27 virtualenv:
26 28   system_site_packages: true
27 29 python:
28 -- "2.7"
30 +- '2.7'
29 31 deploy:
30 - provider: s3
31 - access_key_id: AKIAIGTJF2ZRMYSBAAKQ
32 - secret_access_key:
33   secure: uD0Z3WxSFyHp32ivolx1M3QZ8jcp5E7unQvwFNuFS0oQ1K1HyXIEtnat3HZvwUhTw5cdQc06KYd6/cSUBfy/yRpchXE4Mv6TBXcrvbArSQHAGP/s21bV4
34 - bucket: "rovercode-dev-docs"
35 - local_dir: www/docs/_build/html
36 - upload-dir: rovercode/development
37 - acl: public_read
38 - skip_cleanup: true
39 - region: us-east-2
40 - on:
41   - repo: rovercode/rovercode
42   - branch: docs-deploy
43 - provider: s3
44 - access_key_id: AKIAIGTJF2ZRMYSBAAKQ
```

# NATIVE TOOLS CREATE RISK WITH “ISLANDS OF SECURITY”

## Islands of Security

 Secrets	 Secrets	 Secrets
 Hiera	 Vault	 Databags
 IAM / KMS	 IAM / KMS	 IAM / KMS

- Native tool vendors not focused on security, most not enterprise ready

Vs.

- Central view and control of Privileged Access Security
- Full auditing
- Enterprise wide solution for on-premises, hybrid, cloud only
- Leverage the portfolio of CyberArk capabilities (Vault, monitoring, etc.)

# THE SOLUTION: REMOVE & CENTRALIZE EMBEDDED SECRETS



The diagram illustrates the process of removing embedded secrets from a .gitlab-ci.yml file. A large blue arrow points from the initial state (left) to the final state (right).

**Initial State (Left):** A .gitlab-ci.yml file (117 Bytes) containing the following content:

```
1 trigger_jenkins:
2   variables:
3     INSECURE_JENKINS_PASS: 051cf6a58594c73710492f67
4   script:
5     - './callJenkins.sh'
```

The line `INSECURE_JENKINS_PASS: 051cf6a58594c73710492f67` is highlighted with a red box, indicating the embedded secret.

**Final State (Right):** A .gitlab-ci.yml file (59 Bytes) containing the following content:

```
1 trigger_jenkins:
2   script:
3     - 'summon ./callJenkins.sh'
```

The line `- 'summon ./callJenkins.sh'` is highlighted with a green box, indicating the use of a secret management tool.

**Benefits (Right):** A blue speech bubble lists the benefits of this approach:

- No embedded secrets
- Inject secrets In memory
- Short lived

Demo repo: <https://github.com/quincycheng/cicd/>

# HOW?

## STEP 1: WHERE ARE THEY?



## Cyberark Advanced Threat Landscape - 2018 Report, indicated:

- 75% organizations do not have a privileged account security strategy for DevOps
- Fewer than half report that DevOps and security teams consistently work together
- Nearly all (99%) of security pros and DevOps respondents failed to identify all places where privileged accounts or secrets exist

# CURRENT SITUATION

### CYBERARK GLOBAL ADVANCED THREAT LANDSCAPE SURVEY 2018: FOCUS ON DEVOPS

Unaware and Unprepared: A Lack of Security Awareness and Planning Increases Risk of DevOps Secrets Exposure



CyberArk Global Advanced Threat Landscape

### UNAWARE AND UNPREPARED: DEVOPS SECRETS AT RISK

#### Secrets are Hiding in Plain Sight

Businesses don't understand that privileged accounts and secrets exist across a spectrum of all IT entities.



Nearly all security pro and DevOps respondents failed to identify all places where privileged accounts or secrets exist.

# CREDENTIALS ARE EVERYWHERE (2/2)

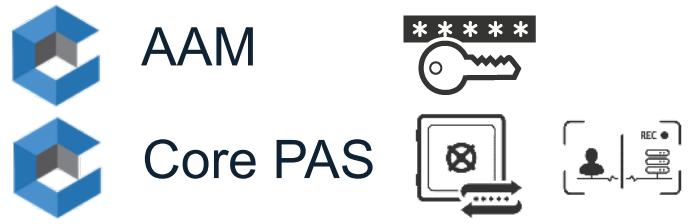


## Target Devices

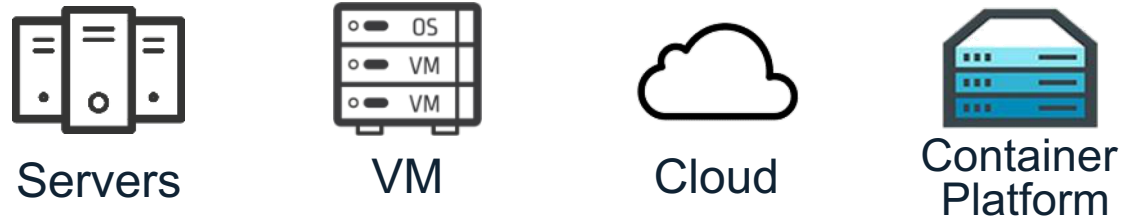


TARGET DEVICES

## Infrastructure as Code



## Infrastructure



**EVERYWHERE! (THAT'S WHY THEY'D BE SECURED IN DAY 1)**





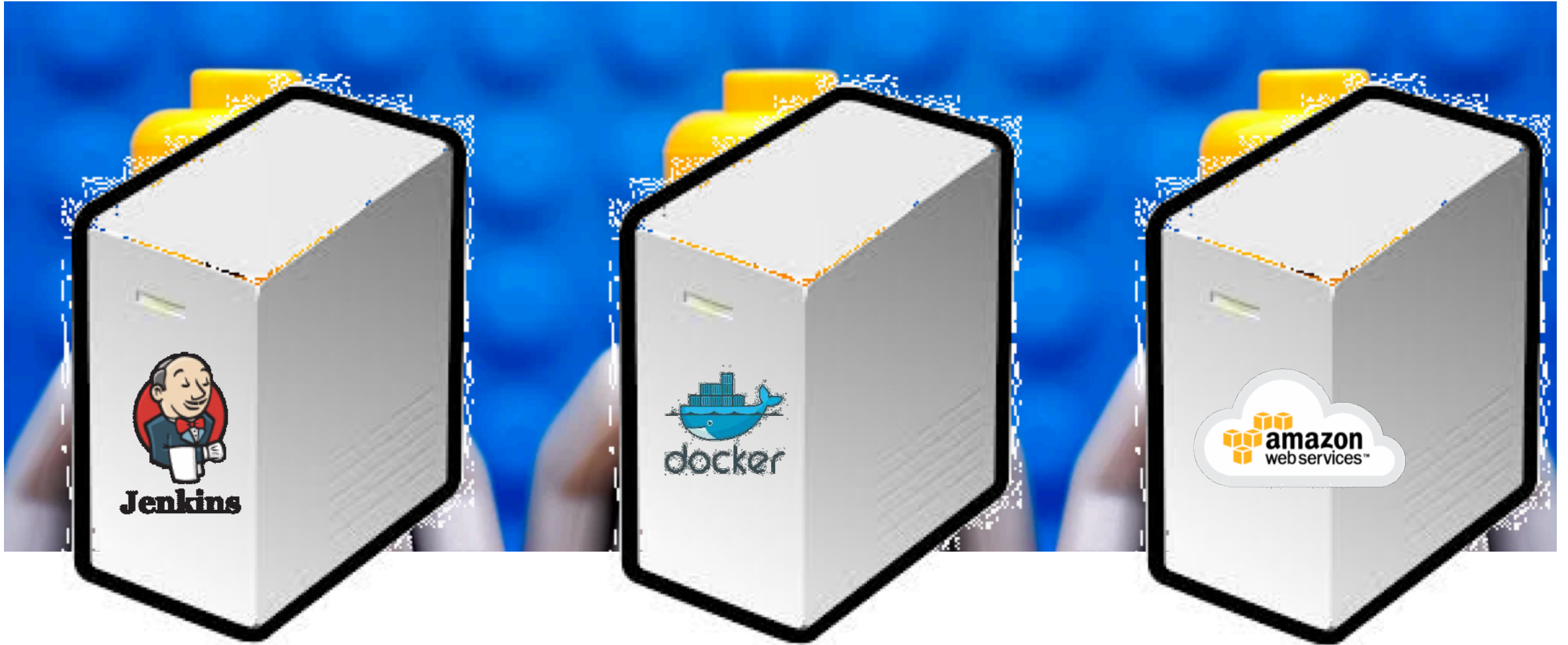
**HOW?**

**STEP 2: LOCK DOWN**

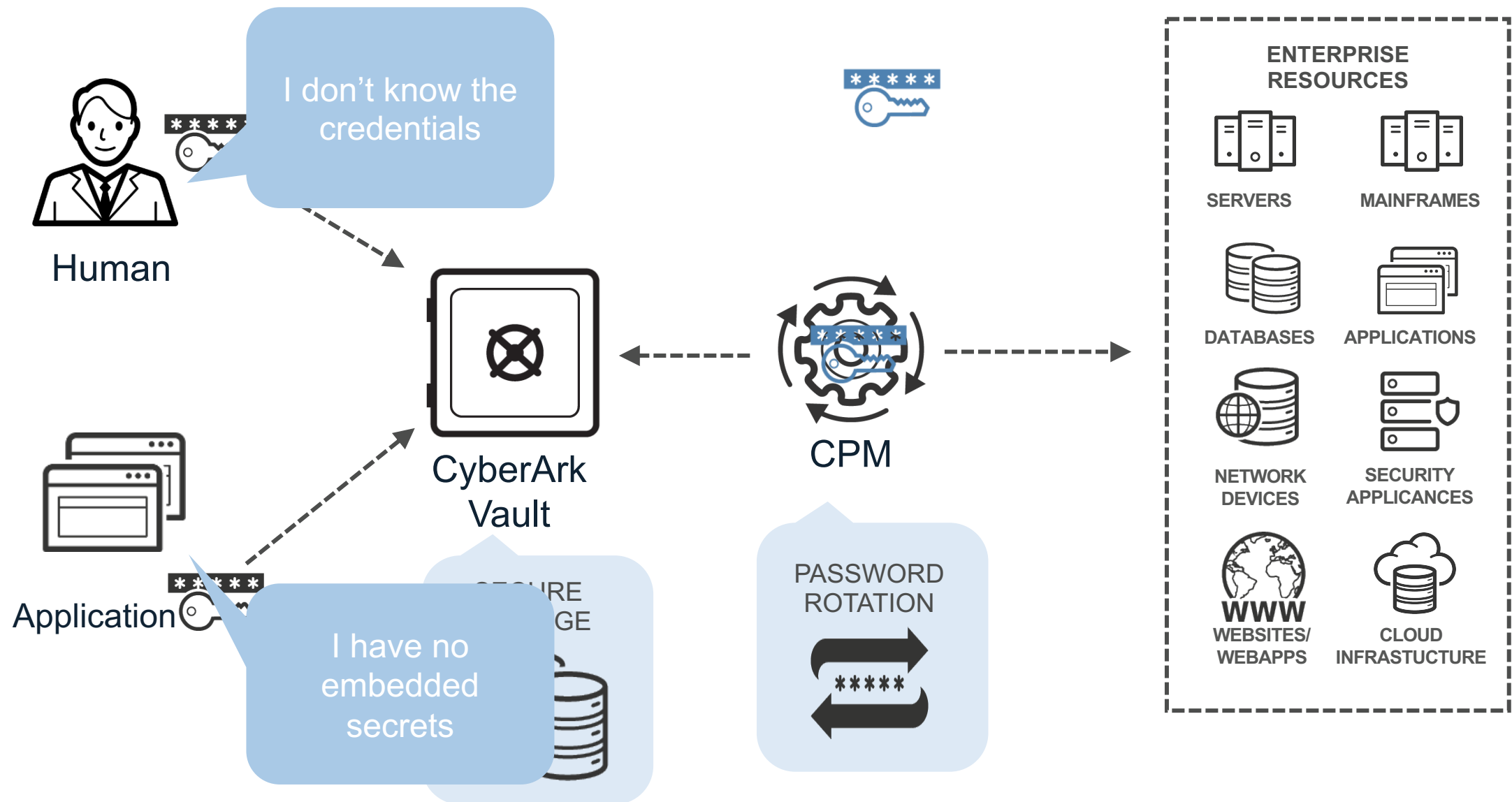


# MACHINE IDENTITY

- Applying Human Security Principles to Machines



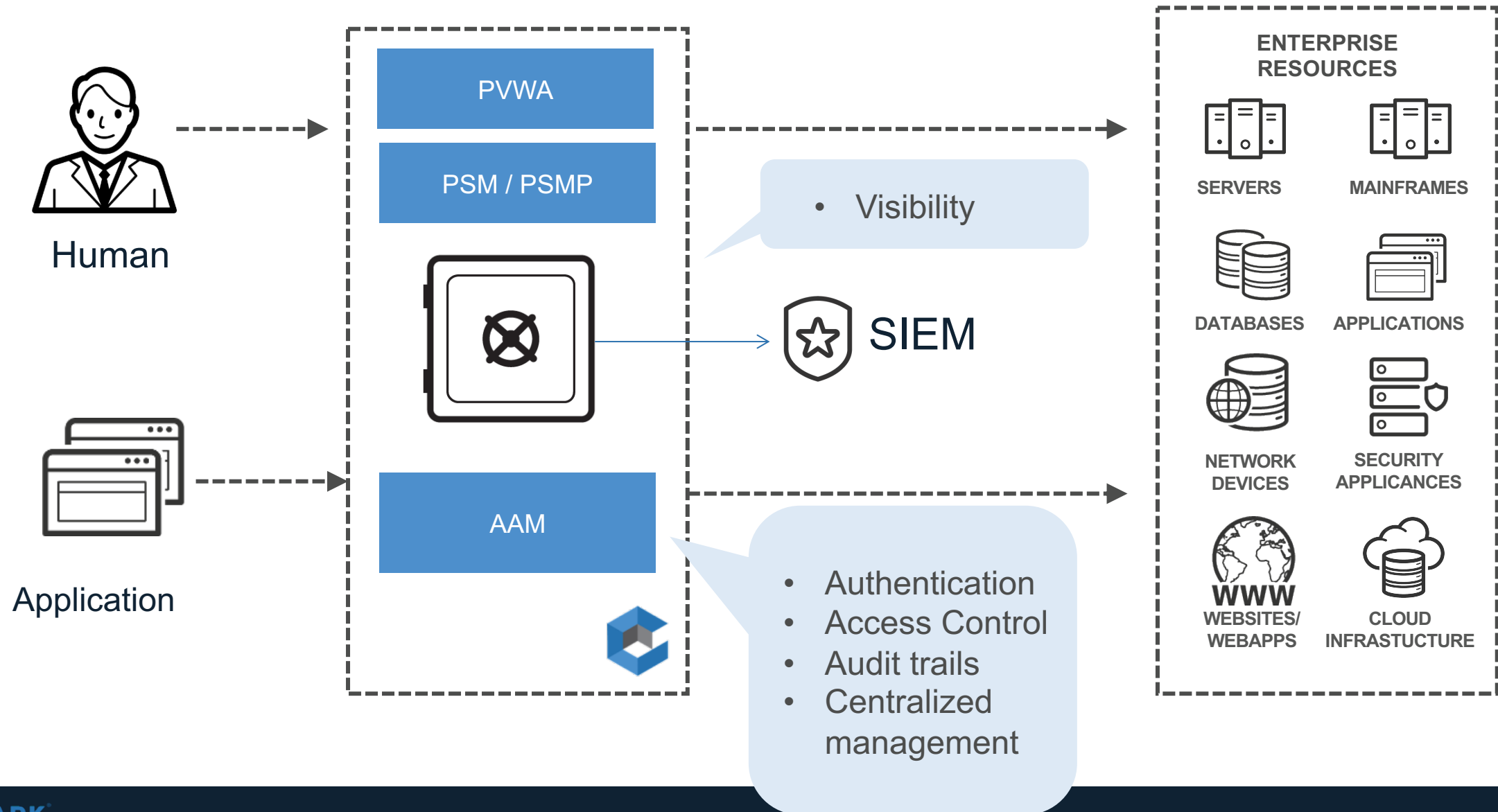
# LOCK DOWN CREDENTIALS



**HOW?**

# **STEP 3: SECURE YOUR SECRETS**

# APPLY SECURITY ENFORCEMENTS

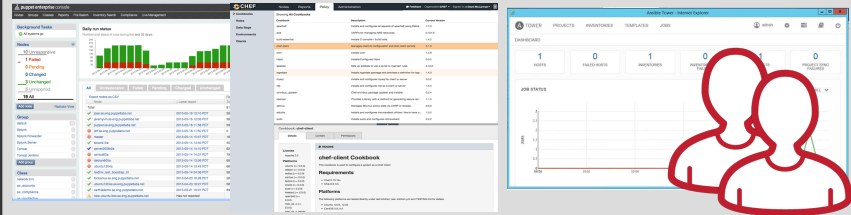




# USE CASE EXAMPLE: PAS & AAM ENABLE END-TO-END SECURITY FOR THE CI/CD PIPELINE

CyberArk's holistic approach secures the full CI/CD Pipeline and Tool Chain end-to-end

## Admin Consoles /Human Users



- ❖ **Protect the tool console**  
Use **Privileged Session Manager** to monitor and record any human or non-human interactive access
- ❖ **Secure the tool credentials**  
Use **Central Policy Manager** to manage and rotate credentials based on policy
- ❖ **Secure the tool CLI**  
Use **On Demand Privilege Manager** to Secure the tool CLI interface
- ❖ **Detect unmanaged & compromised IAM users**  
Use **Privileged Threat Analytics** to detect unmanaged Access Keys, and Passwords for AWS users as well as compromised privileged IAM and EC2 users

PAS and PSM, OPM, PTA

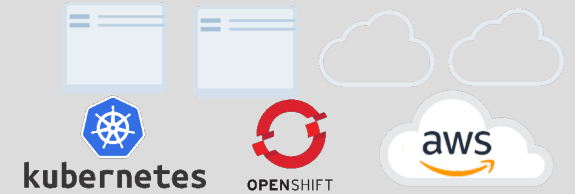
## DevOps CI/CD Pipeline /Automation



- ❖ **Secure the Pipeline credentials**  
Use **Application Access Manager** to manage the credentials used by the pipeline to access resources and run other tools.
- ❖ **Secure Master / Cookbook / Playbook / Manifest / Application containers**  
Use **Application Access Manager** to remove hard coded/ unmanaged credentials from jobs and retrieve them in a secure way
- ❖ **Discover hard coded credentials**  
Use **DNA** to auto-discover hidden credentials in tool Ansible Playbooks, Roles, and Tasks

DNA

## Container /App Deployment



- ❖ **Secure the managed Nodes**  
Use **Application Access Manager** to establish an identity, for containers and other nodes, during orchestration to enable secure retrieval of secrets.
- ❖ **Secure admin access to the Nodes**  
Use **Privileged Session Manager** to secure, control and monitor the access to the nodes

PSM

Application Access Manager: Dynamic Access Provider

# CYBERARK C<sup>3</sup> ALLIANCE & MARKETPLACE

+100 Certified Partners

ab initio

blueprism

APPDYNAMICS

BRANDLE

aqua

aws

atarlabs

Atos

AUTOMATION ANYWHERE

ayehu

B

datablink

Datameer

DATA 443

Data Sunrise

DB NETWORKS

DBmaestro

DBSH

cyber O3SERVER

DEMISTO

DEFACTO

Devolutions

digitate

docker

Duo

EMERGYNT

Eracent

evidian

EZMCOM

FireEye

ForeScout

FLEXERA

FORTINET

GE Power

gemalto

HEXADITE

Hewlett Packard Enterprise

IBM

illusive

Informatika

intel

IP SOFT

iQuate

SONAR

logpoint

LogRhythm

McAfee

okta

Omada

onelogin

OpsRamp

Outpost24

paloalto

Phantom

Pivotal

proofpoint

puppet

Qualys

RADIANT LOGIC

redhat

RAPID7

RSA

SAASPASS

SailPoint

SAP

SECRET DOUBLE OCTOPUS

SECUREAUTH

SECURONIX

serviceNow

SKYBOX SECURITY

splunk

STEALTHbits

StreamSets

SyferLock

Symantec

talend

tenable

THALES

tripwire

Twistlock

UiPath

utimaco

VENAFI

VARONIS

ViSTARa

WorkFusion

WATERFALL

yubico

+100 Certified Joint Solutions

Analytics

Authentication

Detection

DevOps

Discovery

Governance

HSM

ICS

Identity & Access Management

ITSM

Orchestration & Response

Robotic Process Automation

SIEM

Vulnerability Management

+200 Plug-ins

CPM Plug-ins

PSM Plug-ins

CYBERARK

22

# KEY TAKEAWAY

1. NetOps is great if it's secured
2. How CyberArk can help to protect both human credentials and application secrets
3. Contact CyberArk team to help with the evaluation

# THANK YOU!

Quincy Cheng  
APJ DevOps Manager, CyberArk  
[Quincy.Cheng@CyberArk.com](mailto:Quincy.Cheng@CyberArk.com)