Kubernetes 安全防護

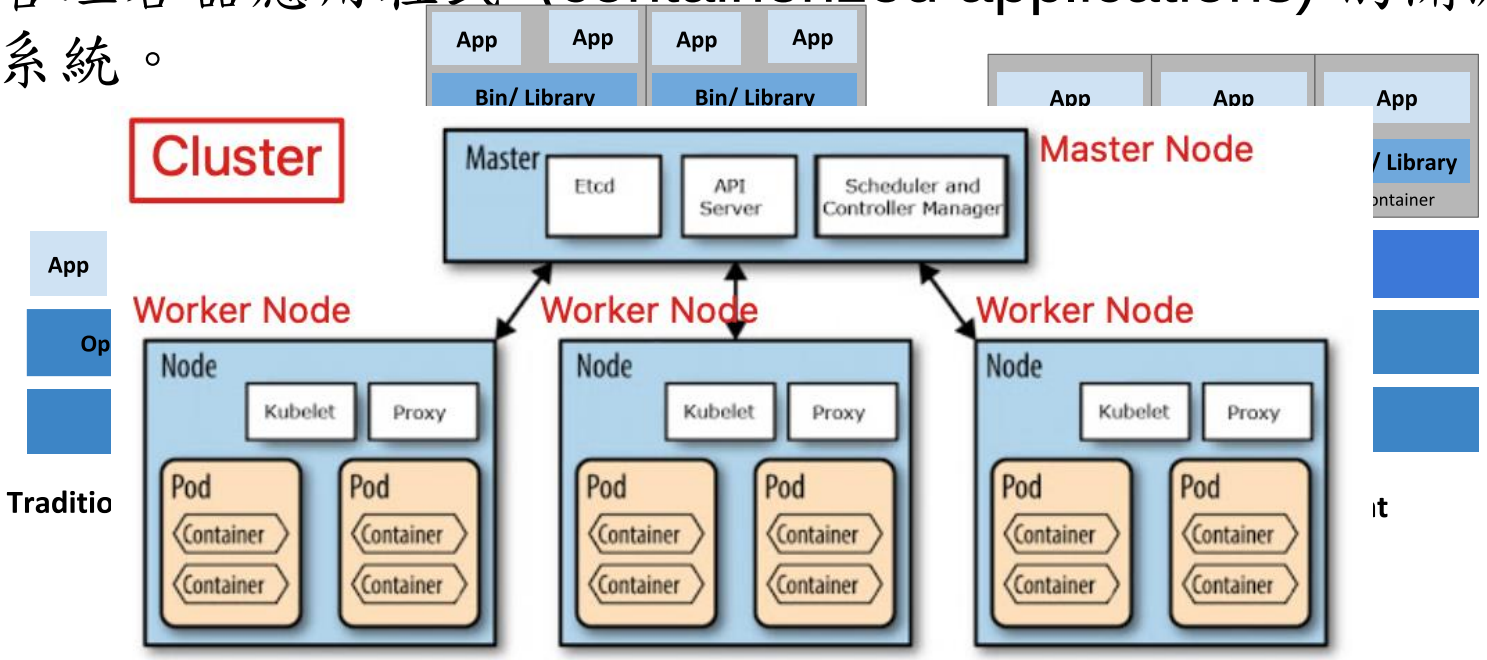
安創資訊股份有限公司
廖建興

大綱

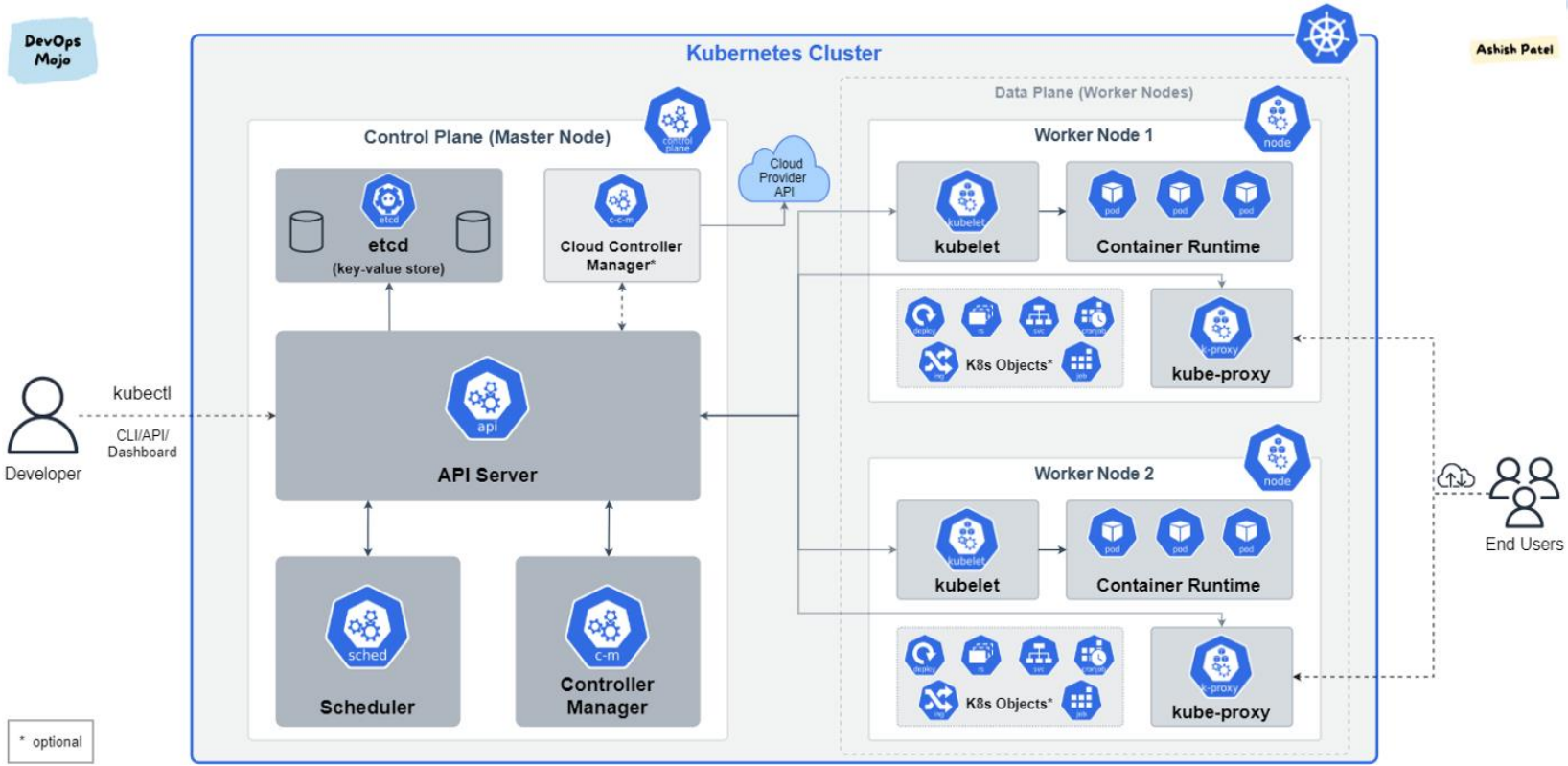
- 什麼是Kubernetes？
- Kubernetes架構與元件
- Kubernetes安全強化
- SentinelOne Singularity Cloud介紹

什麼是Kubernetes?

- Kubernetes 是一種可用來自動化部署、擴充及管理多個管理容器應用程式 (containerized applications) 的開源系統。



Kubernetes 架構與元件



圖片取自：https://medium.com/devops-mojo

Kubernetes 安全強化

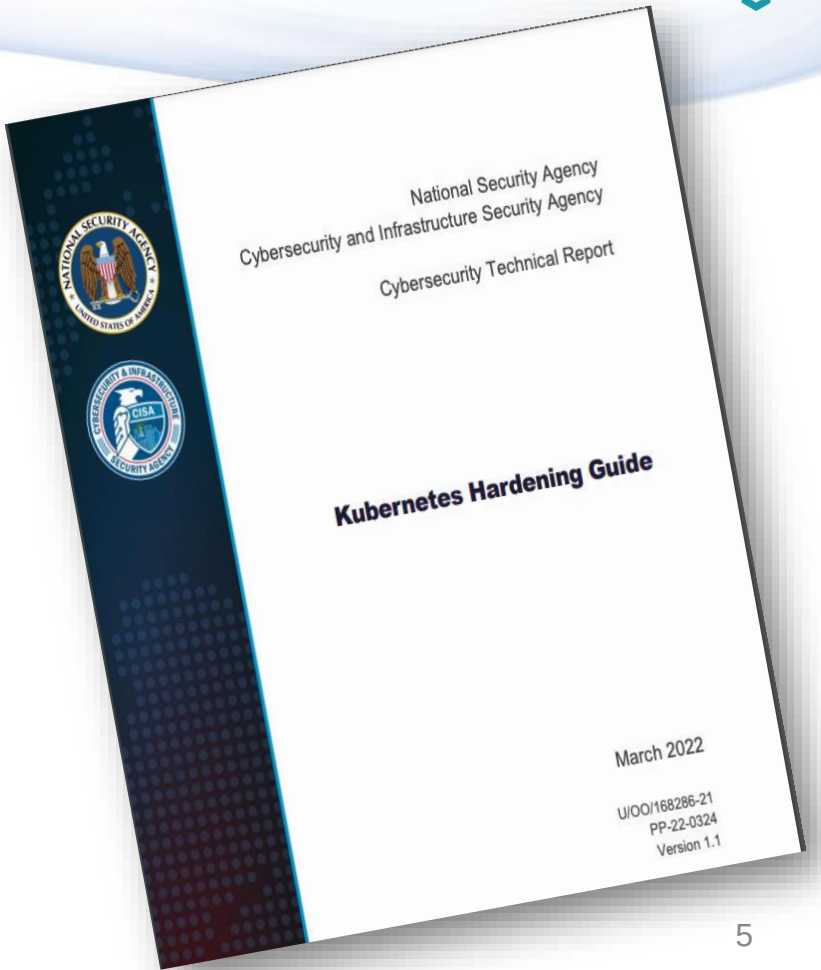
Kubernetes Hardening Guide

- 美國國安局（NSA）與網路安全暨基礎架構安全署（CISA）
- 2021/8/3 共同發表 2022/3/15 更新
- 以下針對三個面向
  提供十個安全強化技巧

➢ Control Plane

➢ Pods & Containers

➢ Telemetry & Threat Detection



強化 Control Plane

1. 分隔網路
   - 使用防火牆限制對 Control Plane 與工作節點的訪問
   - Control Plane 組件和工作節點使用不同網段進行區隔
2. 身份驗證與授權
   - 禁止匿名訪問 (預設允許)
   - 使用基於角色的訪問控制 (RBAC) 策略
   - 非人員使用透過特定服務帳號與令牌授權
   - 最小權限原則
3. 加密通訊
   - 集群內預設未使用加密通訊
   - 使用 Transport Layer Security (TLS) 加密通訊
   - 使用單獨的證書加密 etcd 通訊

強化 Pods & Containers

4. Image 弱點掃描
   - 避免使用不受信任的註冊庫
   - 注意作業系統工具和函示庫弱點
   - Image精簡移除不需要的套件和函示庫
5. 僅在必要時以 root 使用者身份運行
   - 以使用者身份運行應用程式
   - 注意 Kubernetes 設定錯誤會將覆寫使用權限
6. 明確管理 Pod 內部通訊
   - 設置網路策略隔離資源
   - 建立明確的拒絕策略
7. 保護工作負載不變性
   - 使用唯讀文件系統
   - 鎖定容器文件系統防止不當利用

強化 Telemetry & Threat Detection

8. 啟用紀錄
   - 啟用審核日誌記錄（預設禁用）
   - 整個環境配置日誌記錄
9. 日誌聚合和持久化
   - 將日誌收集聚合到集群外
   - 持久化日誌確保在節點、Pod或容器故障的情況下可用
   - 透過外部系統對日誌進行監控與告警
10. 運行時威脅偵測
    - 即時安全修補與更新
    - 定期漏洞掃描與滲透測試
    - 即時偵測防護

➢ 雲防禦深度
   - 運行即時偵測是您的最後一道防線

Singularity™ Cloud

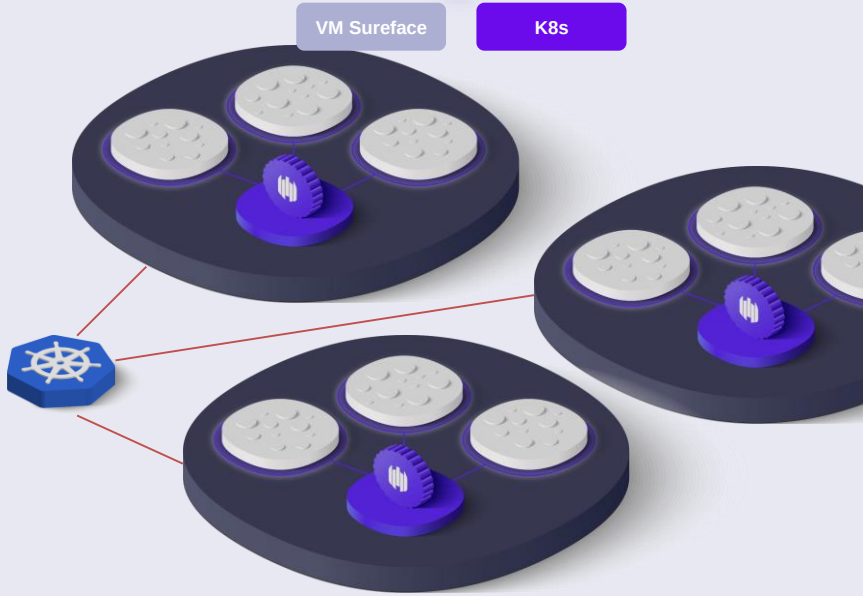
Workload Detection & Response

Singularity Cloud

Kubernetes Workload Detection & Response delivers runtime prevention & EDR for K8s clusters in the cloud and in your data centers.

Outcomes

- **Operational Efficiency** - a single, no-sidecar agent protects the K8s worker, all its pods, and all their containers
- **Operational Simplicity** - Auto-deployed, auto-scaling protection that fits existing DevOps provisioning
- **SecOps Gains Security Visibility for Workloads** - Runtime Prevention + EDR, MITRE ATT&CK mapping, K8s metadata
- **DevOps Maintains the Agility & Stability they expect**. Supports 13 Linux distros with zero kernel dependencies



docker OPENSHIFT aws Azure

Fully Platform & RBAC Integrated

Runtime Prevention + EDR for Workloads

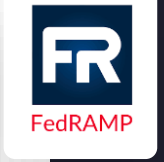
One XDR Data Lake

SE Labs INTELLIGENCE-LED TESTING BEST Innovator WINNER 2021

Singularity Cloud

SentinelOne's strategic partnership with AWS delivers comprehensive visibility and protection for workloads in AWS.

- Singularity on AWS for multi-OS workload coverage, scale, reliability
- Frictionless procurement via the AWS Marketplace through the channel partner of your choice
- Draw down pre-committed AWS Enterprise Discount Program (EDP) spend
- Support for FedRAMP Moderate workloads in AWS GovCloud



- **Public Sector**
- **Security Software Competency**

Runtime EDR with K8s Context

Singularity™ Cloud

K8s Workload Detection & Response

Operational Resilience & Risk Mitigation

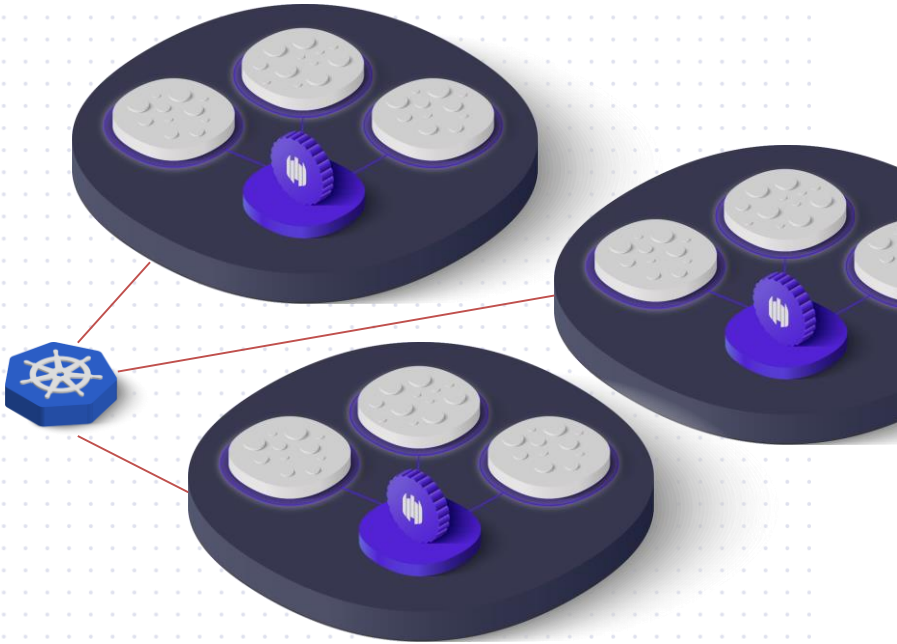
- Runtime protection vs. malware, unknown, & fileless
- ActiveEDR® visibility & hunting inside containers
- **Kill and quarantine threats**, let k8s respawn affected containers
- Full remote shell into pods

Workload Immutability & Agility

- **App Control Engine**: no safelists or ML training

Operational Simplicity

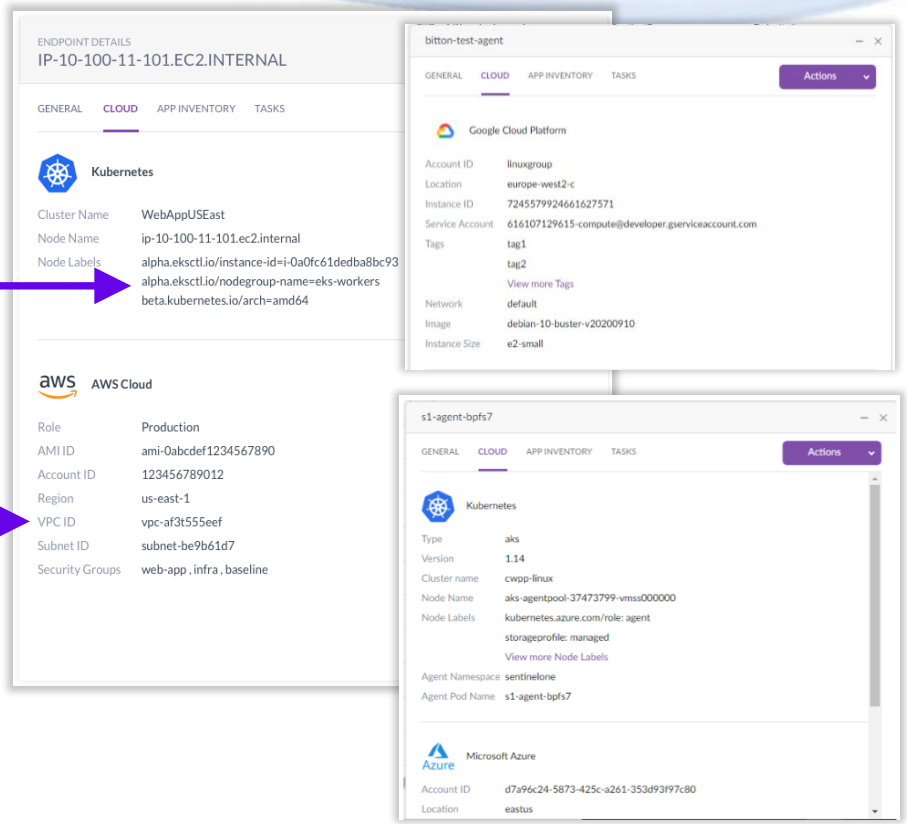
- Auto-deploy via HELM auto-scale as DaemonSet
- 1 agent protects the k8s worker, its pods & containers; NO sidecars
- **User-space agent**: no kernel panics, update OS image at will



Cloud Metadata within S1 Console

- Review VM and K8s metadata tags
  - IDs for machine image, VPC, and more
  - K8s cluster name, worker node name, labels
- Group instances according to tags...
  - account ID
  - AMI ID
  - etc.
- ...and manage groups
  - Apply different policies
  - Monitor resource usage

Ex: EC2 Instance deployed as an EKS worker node.



Demo Video

Securing Kubernetes in Amazon EKS Anywhere

https://www.youtube.com/watch?v=ZwKhZUqxyWY

Thanks!

感謝聆聽