

CYBERSEC 2021

臺灣資安大會

M A Y 4 - 6 臺北南港展覽二館

T R U S T : r e d e f i n e d

信任重構

ORGANIZED BY **iThome**

TrendMicro 2021 CyberLAB



容器安全探討

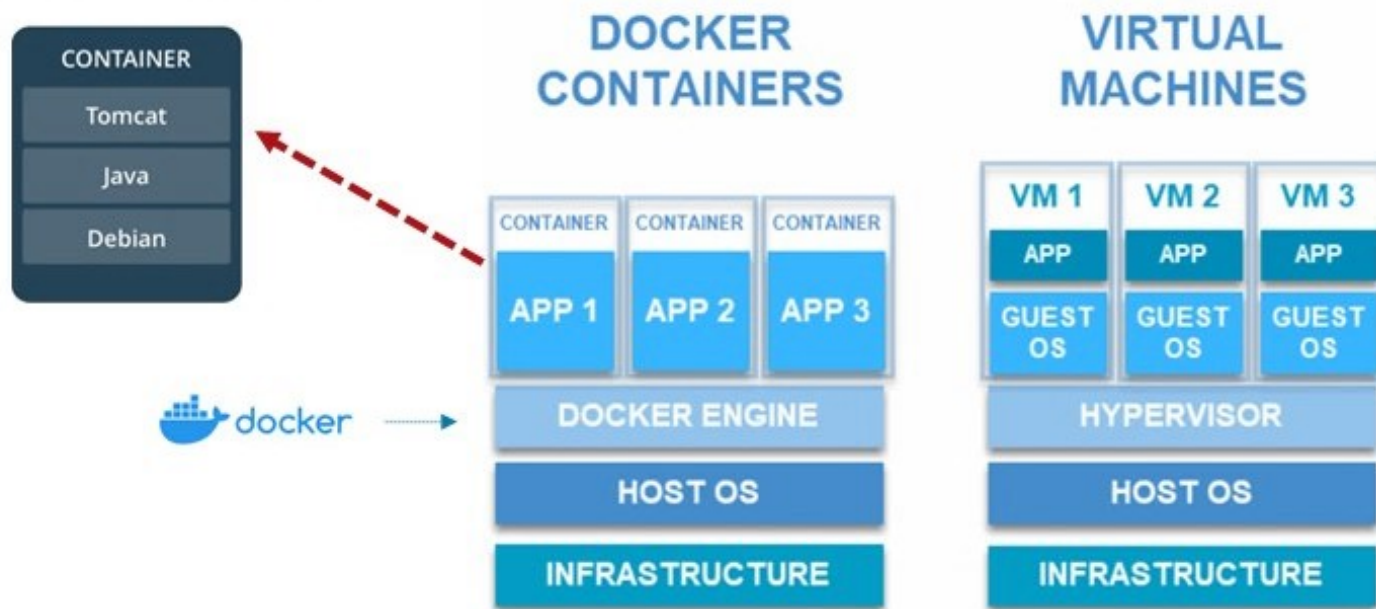


What is a Docker?

- Docker 是一個**開放原始碼軟體**，是一個開放平台，用於開發應用、交付（shipping）應用、執行應用。
- 傳統虛擬化技術如vSphere或Hyper-V是**以作業系統**為中心，而Container技術則是一種**以應用程式**為中心的虛擬化技術。
- Docker 允許使用者將基礎設施（Infrastructure）中的**應用**單獨分割出來，形成更小的顆粒（**容器**），從而提高交付軟體的速度。



VM vs Docker



- 改善傳統**虛擬機器**因為需要額外安裝作業系統 (Guest OS)，導致啟動慢、**佔較大記憶體**的問題
- 以**應用程式**為核心**虛擬化**，取代傳統需要 Guest OS 的**虛擬化技術**

Dockerfile

- FROM jrboys/hol2021:lastest ← 來源
- ADD ROOT.tar /usr/local/tomcat/webapps
- ADD showcase.tar /usr/local/tomcat/webapps

```
Step 1/3 : FROM jrboys/hol2021
--> 94eedb9b8de2
Step 2/3 : ADD ROOT.tar /usr/local/tomcat/webapps
--> 59bc737cd029
Step 3/3 : ADD showcase.tar /usr/local/tomcat/webapps
--> 83c64cb43936
Successfully built 83c64cb43936
```



What is kubernetes?

container-orchestration system for
automating application deployment,
scaling, and management wikipedia



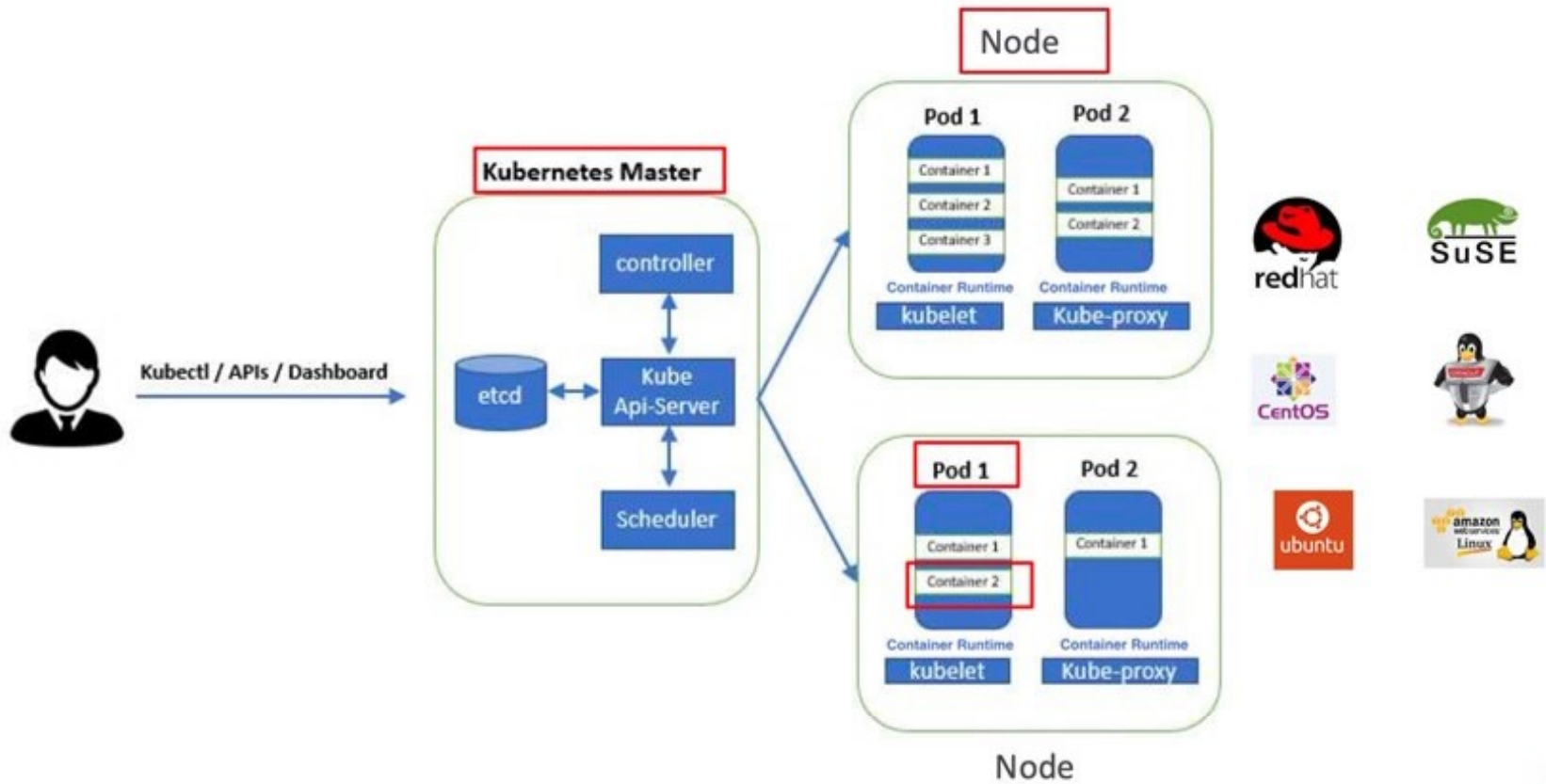
Docker VS Kubernetes



救人、接炸彈、談判、秘密遣入
接住大樓、飛很高、快速移動



Kubernetes for Central Management



你用的image安全嗎？

包含加密貨幣支援惡意軟體的多種Docker映象，已經由Docker Hub大量擴散

時間 2020-06-25 23:13:46 DockOne

語言: [CN](#) / [T](#)

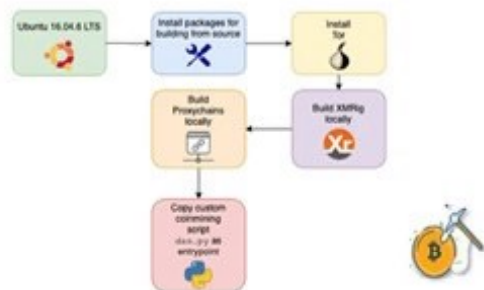
主題: [Docker](#) [集線器](#)

資料來源：<https://www.mdeditor.tw/pl/pyen/zh-tw>



事件概要：

- Docker 帳戶：azurenql
- 問題image：包含234_122等6個image
- 攻擊手法：利用容器啟用時，自動執行以下功能：
 - 安裝Tor
 - 安裝XMRig
 - 安裝ProxyChains
 - 執行定制化的dao.py進行挖礦



```
"Entrypoint": [  
    "/bin/sh",  
    "-c",  
    "python /etc/dao.py"  
],
```

程式開發人員會下載到嗎？



azurenl

Community User • Joined October 15, 2019

Repositories Starred

Displaying 8 of 8 repositories

azurenl/227_135 By azurenl • Updated 5 months ago Container	500K+ Downloads
azurenl/234_122 By azurenl • Updated 6 months ago Container	500K+ Downloads
azurenl/53_57 By azurenl • Updated 6 months ago Container	1M+ Downloads
azurenl/93_164 By azurenl • Updated 7 months ago Container	500K+ Downloads
azurenl/227_135_app By azurenl • Updated 7 months ago Container	8.1K Downloads
azurenl/227_135_tor By azurenl • Updated 7 months ago	6.1K Downloads

下載50萬次

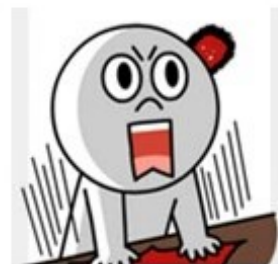
下載50萬次

下載100萬次

下載50萬次

下載14萬次

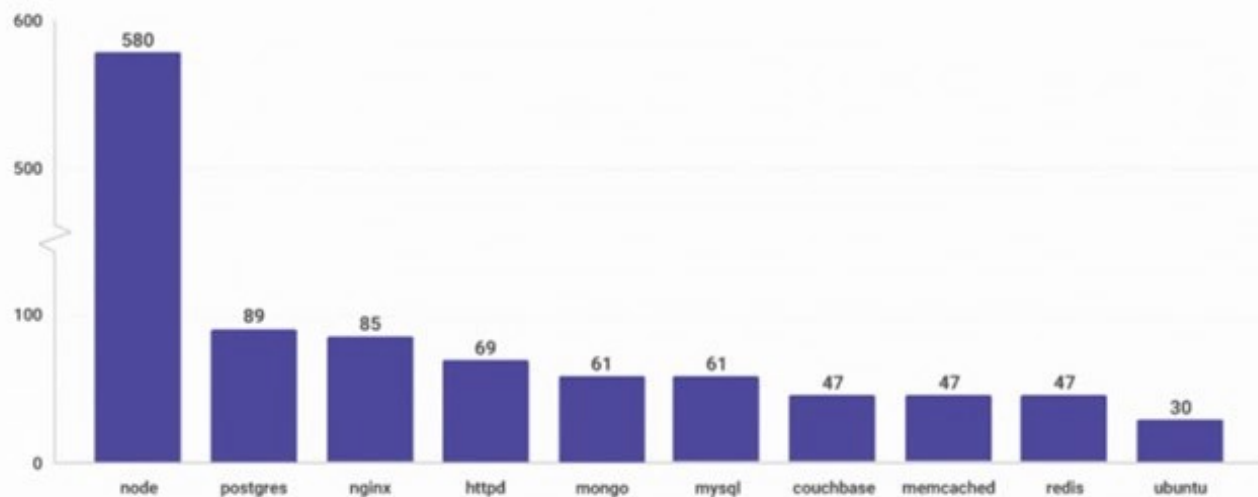
合計200萬次



報告：前十大熱門Docker映像檔都有至少30個以上的漏洞

Snyk掃描Docker Hub中最多開發者使用的Docker映像檔，發現官方的Node.js映像檔含有580個易受攻擊的系統函式庫

Number of OS vulnerabilities by docker image



資料來源：<https://www.ithome.com.tw/news/129018>

【開源陷阱】 Docker Hub 400萬images過半有漏洞 開發團隊貪快變內鬼

By Wepro180 小編 — 最後更新於 Dec 8, 2020

科技傳訊

公認有助加快 DevOps 流程的 Container 容器技術，其最受歡迎開發平台 Docker Hub 被驗出含有大量惡意 Images，400 萬個 images 當中超過一半有問題，只要開發團隊隨意下載這些開源 images 使用，隨時無意中成為入侵幫兇.....

Docker 虛擬化技術深受應用程式開發者歡迎，因為可將應用程式連同環境製作成不同的 Image，快速移植到各種作業系統之上。雖然 Image 一經封裝，理論上便不可改變，但並不代表 Container 絕對安全，因為黑客可以將「加料」Image 放在開源 (Open Source) 倉庫上，待開發人員下載使用。

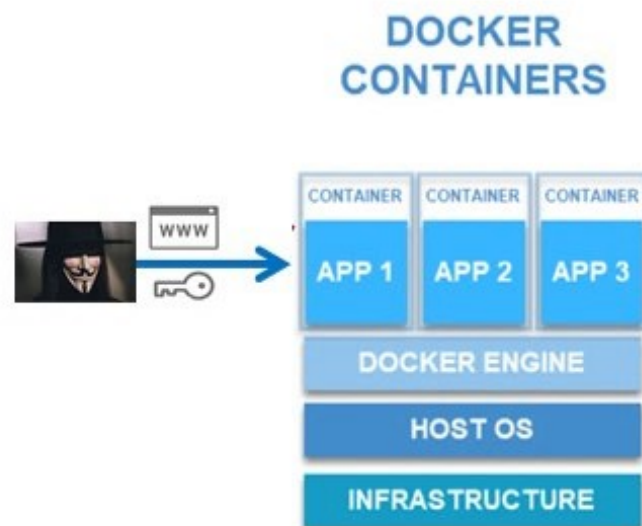
以為危言聳聽？最近專門提供 Container 安全服務的公司 Prevasio，就有研究報告話俾大家知 Container 有多危險。Prevasio 研究員利用 800 個電腦設備，連續一個月不停掃描存放於 Docker Hub 上的開源 Container Images 後，發現 400 萬個 Images 中超過一半含有安全漏洞，當中 13% 屬於高風險級別。另外，有 6,400 個 Images 更被界定為含有惡意功能，包括礦、木馬程式等等，只要有開發團隊未經檢查分析而直接使用，就會一併引入漏洞及惡意軟件。

資料來源：<https://wepro180.com/tech-news/%E3%80%90%E9%96%8B%E6%B8%A%90%E9%99%B7%E9%98%B1%E3%80%91docker-hub-400%E8%90%ACimages%E9%81%8E%E5%8D%8A%E6%9C%89%E6%BC%8F%E6%B4%9E-%E9%96%8B%E7%99%BC%E5%9C%98%E9%9A%8A%E8%B2%AA%E5%BF%AB%E8%AE%8A/>



2021 Cyber Lab

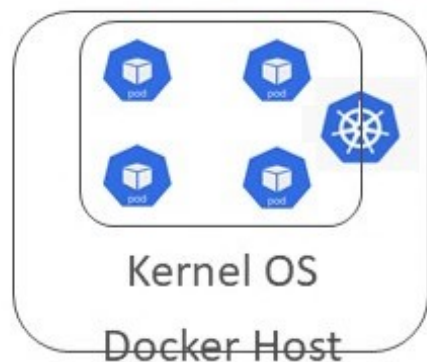
- Lab 1: Create your own container
- Lab 2: Container hacking
- Lab 3: Vulnerability protect
- Lab 4: Admission control



Kubernetes 開發階段威脅



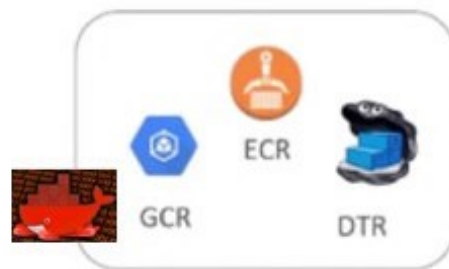
Kubernetes 佈署階段威脅



```
containers:  
- name: mylab  
  image: '0000000000/albert:mylab'  
  ports:  
  - containerPort: 8080  
  securityContext:  
    privileged: true
```



Pull image



1. 特權容器佈署
2. 特權容器可存取host系統檔案
3. 無法確認image是否安全
4. CI/CD自動化，無法保證安全

Kebernetes 資安該考慮的

1. 如何確保開發人員皆使用安全無虞的印像檔(image)
2. 印像檔內所使用的open source版本是否為新版
3. 如何阻止開發人員有意無意的特權容器派送
4. 容器是否符合公司或國際法規政策



Container Security

Trend Micro Cloud One™

Security Services Platform for Cloud Builders



Cloud Security Simplified

Container Security 功能

進階映像掃描:

- 偵測惡意程式。
- 評估漏洞。
- 搜尋Application是否含有機敏資料，如私密金鑰和密碼。
- 政策遵循(PCI-DSS, HIPAA, and NIST 800-190)。
- 使用 Snyk 偵測原始程式碼及版本漏洞。

Container Security 功能

自動化流程防護:

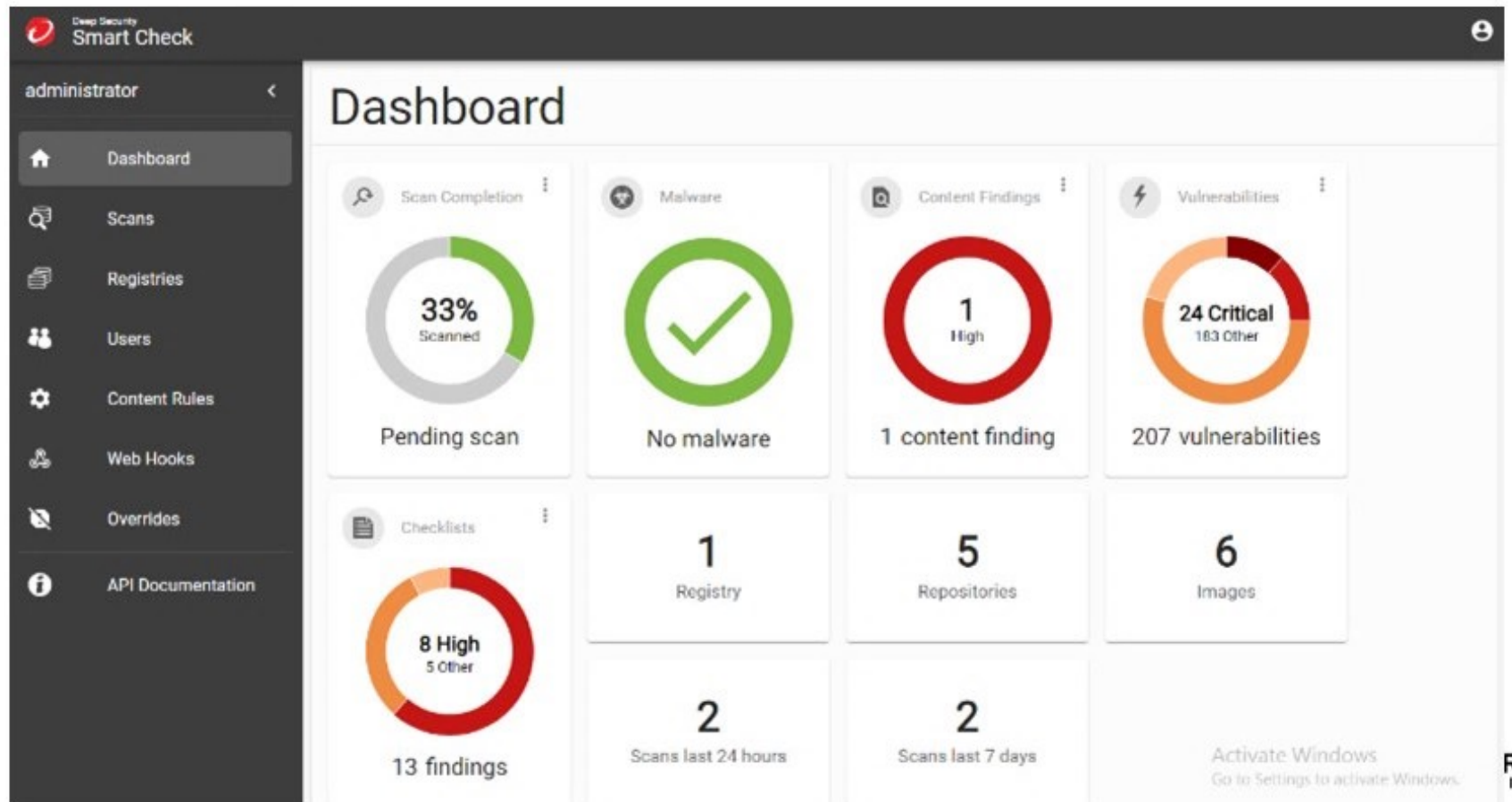
- 當有映像推送至 Docker 登錄當中時，您的 CI/CD 系統就可自動呼叫 **Container Security API** 來啟動掃描，並透過 API 來取得掃描結果。
- Container Security API 也內含了 Webhook 機制來讓 CI/CD 元件註冊接收掃描事件通知，例如「掃描完成」(scan-completed) 通知，方便將工作流程自動化。

Container Security 功能

貫徹法規遵循:

Container Security 提供進階的遵規掃描，藉由客製化的政策來確保您達成內部和外部要求。Container Security 的掃描記錄可滿足業務與稽核要求，提供詳細的掃描歷史記錄和結果。

SmartCheck UI



image掃描結果

Layers



|7 BASE_URL=https://downloads.apache.org GID=1000 MIRROR_BASE_URL=https://downloads.apache.org NIFI_BINARY_PATH=/nifi/1.12.1/nifi-1.12.1-bin.zip NIFI_TOOLKIT_BIN_



|7 BASE_URL=https://downloads.apache.org GID=1000 MIRROR_BASE_URL=https://downloads.apache.org NIFI_BINARY_PATH=/nifi/1.12.1/nifi-1.12.1-bin.zip NIFI_TOOLKIT_BIN_



RUN set -eux; apt-get update; apt-get install -y --no-install-recommends bzip2 unzip xz-utils ca-certificates p11-kit fontconfig libfreetype6 ; rm -rf /var/lib/a_

Layer ID: sha256:ffba832277c8663ab5396dede4444669c60d1be8adc401d40f4f65b716b1e26d

Created at:

2020-08-05 08:45

Created with:

```
RUN set -eux; apt-get update; apt-get install -y --no-install-recommends bzip2 unzip xz-utils ca-certificates p11-kit fontconfig libfreetype6 ; rm -rf /var/lib/apt/lists/
```

Vulnerabilities:

Legend:

🔍 Fix available in newer version

Package/Module	Severity	Vulnerabilities
libpng1.6 1.6.30-6	High	CVE-2018-14550
	Medium	CVE-2018-14048 , CVE-2019-6129
expat 2.2.6-2+deb10u1	Medium	CVE-2013-0340
freetype 2.9.1-3+deb10u1	Medium	🔍 CVE-2020-15999

Privileged container Control

Trend Micro Cloud One™ > Container Security ▾ Sign out Help ▾

Admission Policies

[+New](#) [+Duplicate](#)

Name	Description	Created	Updated	
admission_poc_policy		2020-12-13 16:36	2020-12-13 17:32	
admission_policy_deny_root_contain		2020-12-17 10:42	2020-12-17 10:42	

Name
The policy name cannot be changed after the policy has been created.

Description

Policy action

Rules

Pod properties

- Containers that **run as root** ⓘ
- Containers that **run in the host network namespace** ⓘ
- Containers that **run in the host IPC namespace** ⓘ
- Containers that **run in the host PID namespace** ⓘ

Container properties

- Containers that **run as root** ⓘ
- Privileged** containers ⓘ
- Containers with **privilege escalation** rights ⓘ
- Containers that can **write to the root filesystem** ⓘ

驗證YAML 檔

- 判斷設定皆符合規範才能佈署

Control Aspect	Field Names
Running of privileged containers	<code>privileged</code>
Usage of host namespaces	<code>hostPID</code> , <code>hostIPC</code>
Usage of host networking and ports	<code>hostNetwork</code> , <code>hostPorts</code>
Usage of volume types	<code>volumes</code>
Usage of the host filesystem	<code>allowedHostPaths</code>
Allow specific FlexVolume drivers	<code>allowedFlexVolumes</code>

Admission Control Event

Admission Events

Filter by: Cluster Action: Block

Action	Time	Admission Policy	Cluster	Namespace	Operation	Kind
Block	2020-12-17 08:04	admission_poc_policy	albert_cluster2	default	Create	Job
Block	2020-12-17 08:04	admission_poc_policy	albert_cluster2	default	Create	Job
Block	2020-12-17 08:04	admission_poc_policy	albert_cluster2	default	Create	Job
Block	2020-12-17 08:04	admission_poc_policy	albert_cluster2	default	Create	Job
Block	2020-12-17 08:04	admission_poc_policy	albert_cluster2	default	Create	Job
Block	2020-12-17 08:04	admission_poc_policy	albert_cluster2	default	Create	Job
Block	2020-12-17 08:03	admission_poc_policy	albert_cluster2	default	Create	Job
Block	2020-12-17 08:03	admission_poc_policy	albert_cluster2	default	Create	Job
Block	2020-12-17 08:03	admission_poc_policy	albert_cluster2	default	Create	Job
Block	2020-12-17 08:03	admission_poc_policy	albert_cluster2	default	Create	Job

Time: 2020-12-17 08:04 Admission Policy: admission_poc_policy **規則名稱**

Action: **Block** **處理動作** Operation: Create

Decision: Deny Kind: Job

Cluster: albert_cluster2

Namespace: default

Policy violations

Object	Image	Container	Findings
Images that are not scanned ⓘ			
scan-1608163200	deepsecurity/tasks@sha256:a507f0b72be51fb746c0280724db57fd532957586a5107f00de5881e362170ca	tasks	

完整 API 整合CI/CD

Scans

Ongoing and historical scans

List scans

Retrieve a list of scans. Scans are returned in descending order of creation time, so the latest scan is returned first.

AUTHORIZATIONS token

QUERY PARAMETERS

expand	string Default: <code>"all"</code> Enum: <code>"all"</code> , <code>"none"</code> A comma-separated list of attributes to expand in the results.
cursor	string <byte> Default: <code>""</code> An encoded value used to retrieve the next set of results for a query that returns more than <code>limit</code> results.
limit	integer <int32> Default: <code>25</code> The maximum number of records to return.
repository	string When present, the <code>repository</code> query parameter will filter the list of scans to those scans where the <code>source.repository</code> contains the provided value. If the <code>exact</code> query parameter is also provided (and <code>true</code>), the filter will do an exact match on the value.
repository	string When present, the <code>repository</code> query parameter will filter the list of scans to those scans where the <code>source.repository</code> contains the provided value. If the <code>exact</code> query parameter is also provided (and <code>true</code>), the filter will do an exact match on the value.
tag	string

REST Client

GET /api/scans

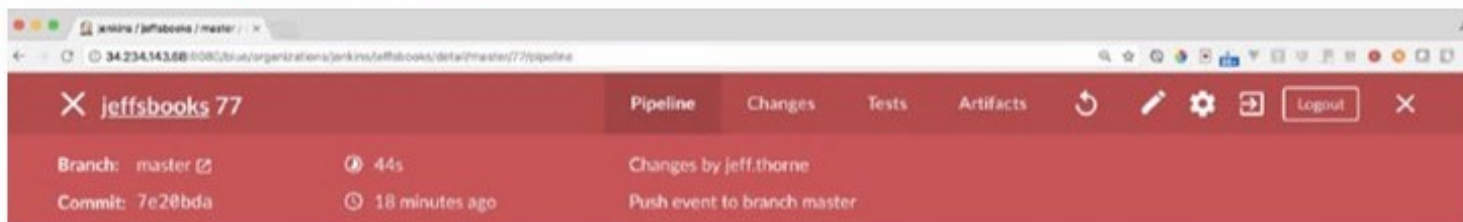
Response samples

200 400 401 500 503

Content type: application/json

```
{
  "scans": [
    + ( - )
  ],
  "next": "493pcy827Fs1220pcy8vo0Pz4W0s10R1Y2Rka9Sa000084H4L8103110Pz0C0"
}
```

Jenkins CI/CD 整合



佈署阻擋

Initiate Trend Micro SmartCheck Container Image Assurance Scan - 32s

python3 /home/ubuntu/jenkins_plugin.py -- Shell Script 32s

```
1 [jeffsbooks_master-YRGTSEU6W9MJDASF5IF27BL7VHLMFPMQBSYX7P4VEYABVXQBLYLULO] Running shell script
2 + python3 /home/ubuntu/jenkins_plugin.py
```

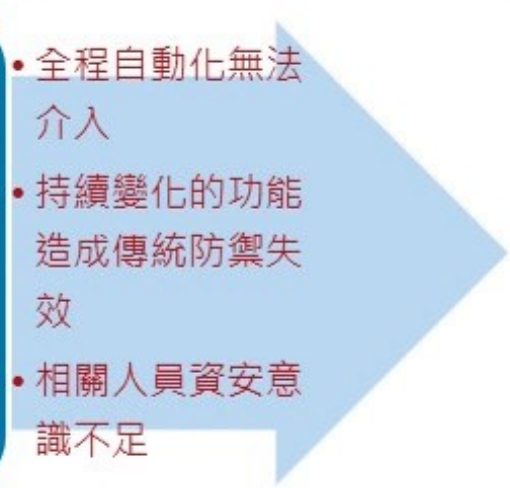
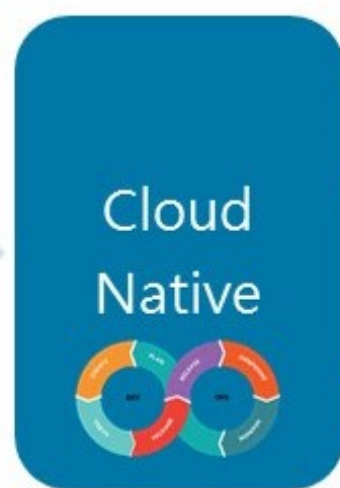
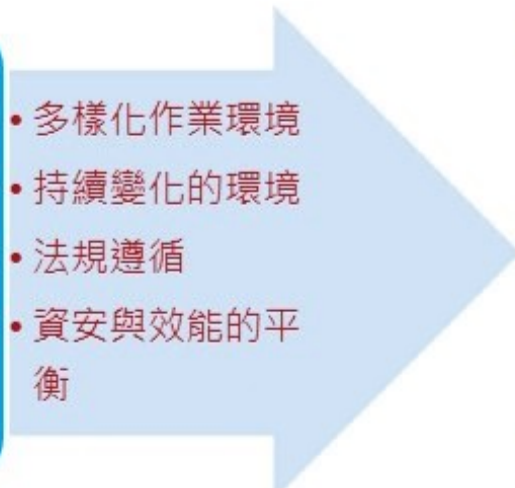
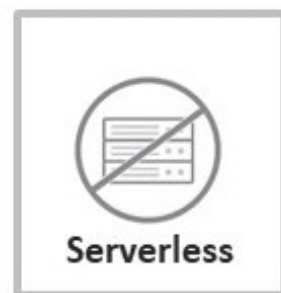
```
root@ip-172-31-27-247:/home/ubuntu# kubectl apply -f busybox.yaml
Error from server: error when creating "busybox.yaml": admission webhook "trendmicro-admission-controller.default.svc" denied the request: - containerSecurityContext violates rule "privileged" in container(s) "busybox-container".
```

偵測特權容器



其實～雲端保護還需要更多

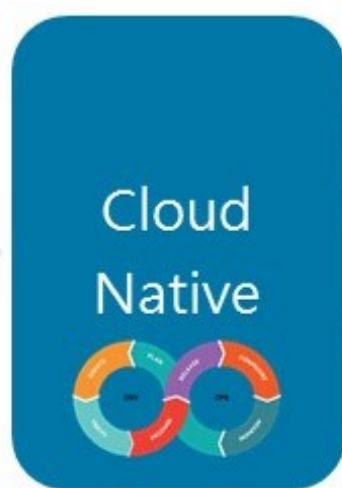
雲端化資安人員面臨的挑戰



雲端化面臨的資安威脅



- 系統漏洞攻擊
- 應用程式弱點攻擊
- 網路弱點攻擊
- 惡意程式感染



- 錯誤的容器組態
- 含有漏洞的原始碼
- CI/CD開發管道規畫缺失

雲端資安務實作法



On-premise



Public Cloud



Container



Serverless

法規遵循

持續檢查

自動修復

攻擊防禦

多平台支援

全方位防禦

自動擴展

開發安全

融入開發流程

弱點矯正

執行中防禦

單一管理平台

Trend Micro Cloud One™

Security Services Platform for Cloud Builders



Cloud Security Simplified



Thank You

