CYBERSEC 2025 臺灣資安大會 | 4/15-4/17 臺北南港展覽二館

CLOUD SECURITY Forum

CLOUD SECURITY FORUM

K8s 與容器服務攻擊手法 層出不窮，企業如何防禦？

TEAM CYBERSECURITY

Aspen Yang

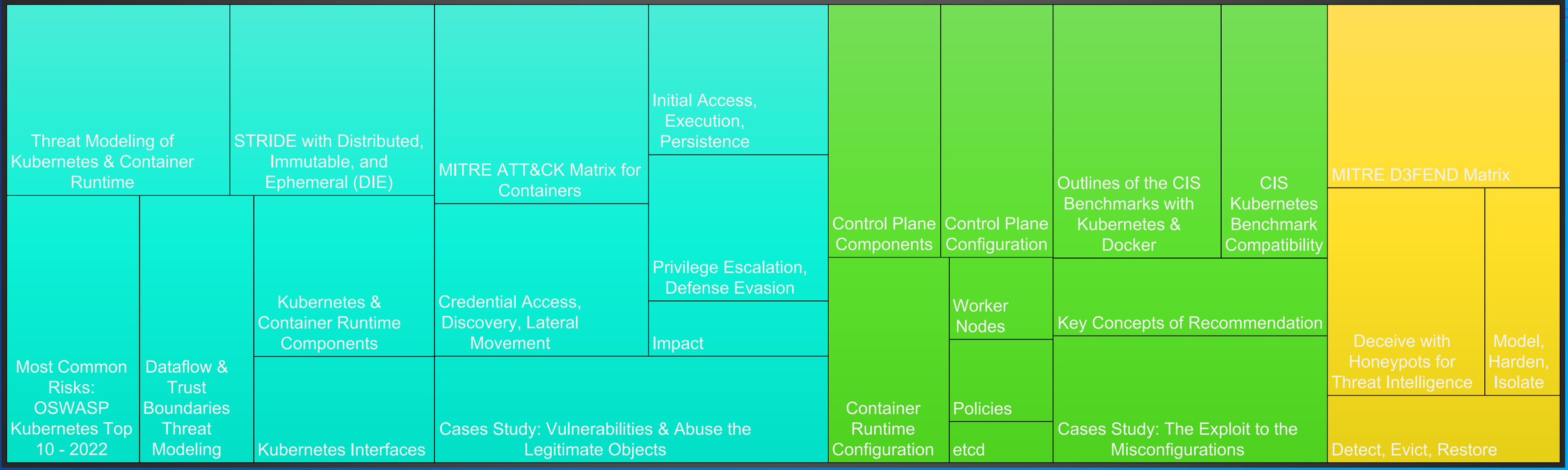
敦陽科技 | Stark Technology Inc.

雲端應用部 技術經理

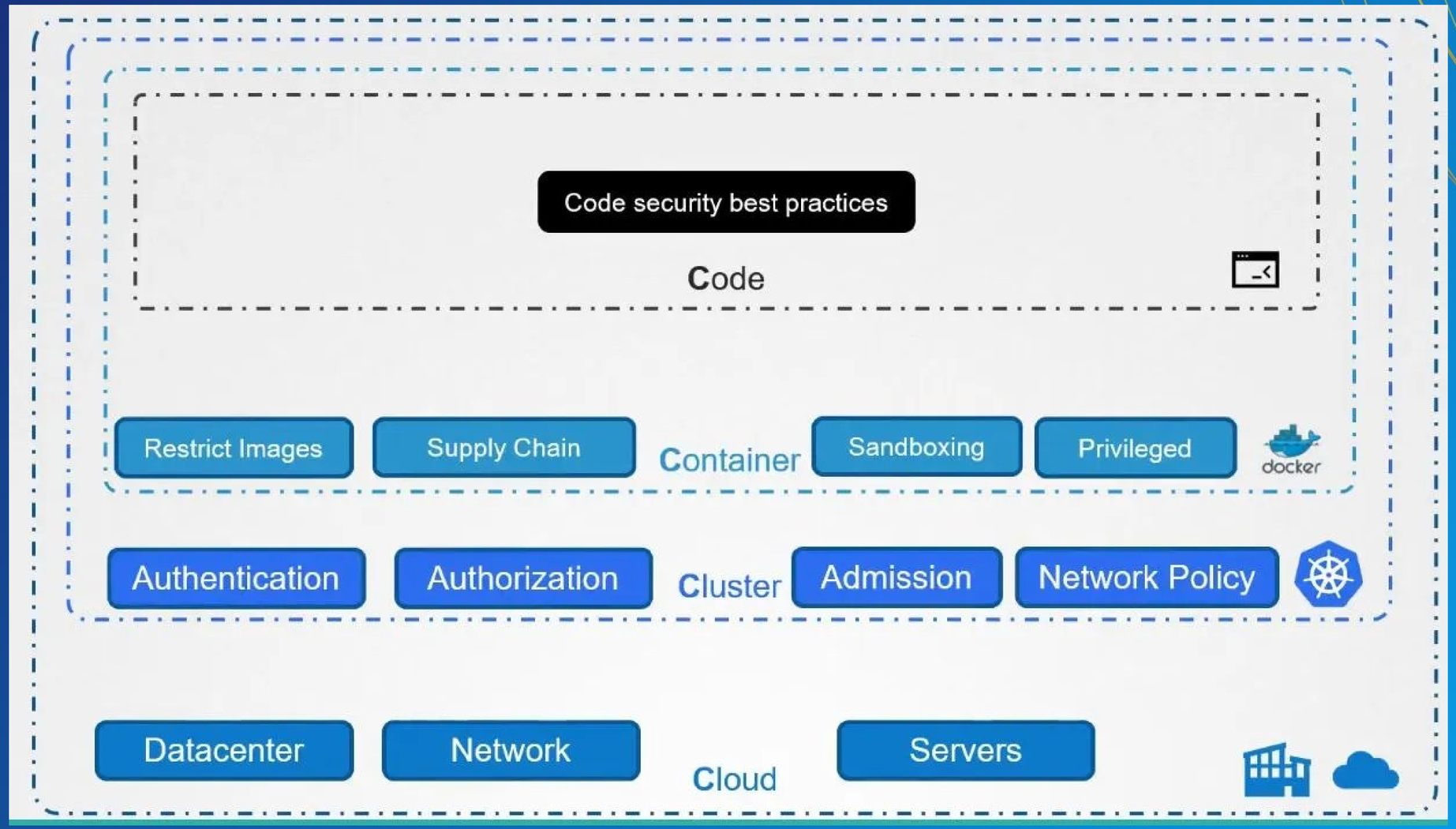
Agenda

AGENDA

- Prologue (導言)
- Adversary Driven Security (攻擊者驅動資安)
- Audit Driven Security (稽核驅動資安)
- Defending Kubernetes: Best Practices & Controls (防護 Kubernetes：最佳實務與控制措施)
- Summary (總結)



Prologue



Ref: Understanding the Kubernetes Attack Surface - Jon Goldman

Adversary Driven Security (攻擊者驅動資安)

攻擊者驅動資安
Adversary Driven Security
Kubernetes 與 Container Runtime 之威脅建模
Threat Modeling of Kubernetes & Container Runtime
容器化的 MITRE ATT&CK 矩陣
MITRE ATT&CK Matrix for Containers
攻擊情境案例研究：弱點與濫用
Cases Study: Exploitable Vulnerabilities & Abuse the Legitimate Objects
稽核驅動資安
Audit Driven Security
理解CIS Kubernetes與Docker的評測基準
Outlines of the CIS Benchmarks with Kubernetes & Docker
CIS評測: 稽核缺失即錯誤設定
CIS Benchmarks: Audit Deficiencies as Misconfigurations
攻擊情境案例研究：錯誤設定
Cases Study: The Exploit to the Misconfigurations
防禦 Kubernetes
Defending Kubetnetes
使用MITRE D3FEND矩陣 將最佳實踐與控制措施加以分類
Mapping the Best Practices & Controls to MITRE D3FEND Matrix

Concepts of Threat Modeling

Threat Modeling Manifesto:

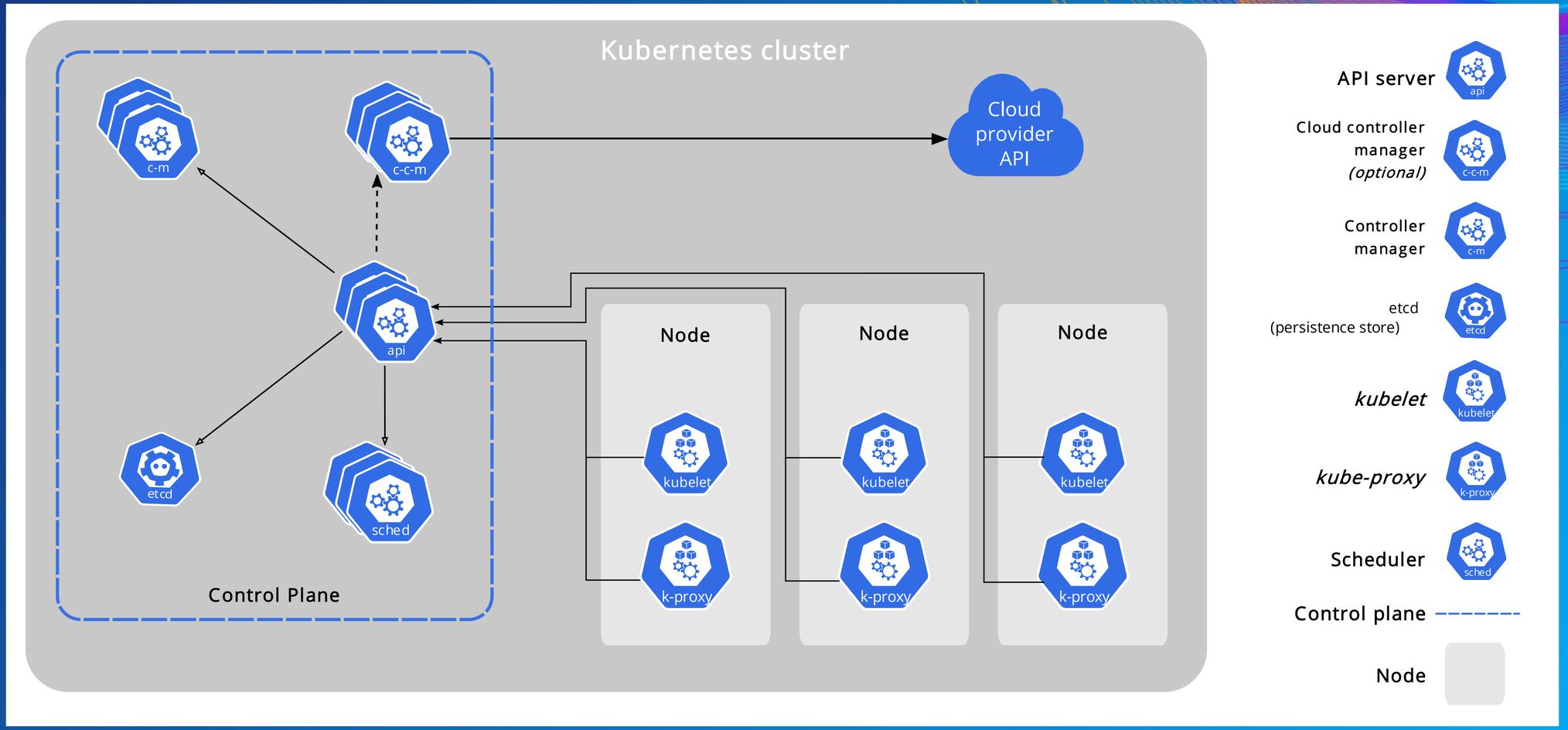
- ✓ What are we working on?
- ✓ What can go wrong?
- ✓ What are we going to do about it?
- ✓ Did we do a good enough job?

This allows security to be "built-into" a system rather than "bolted-on“.

- OWASP: Threat Modeling Cheat Sheet

Kubernetes & Container Runtime Components

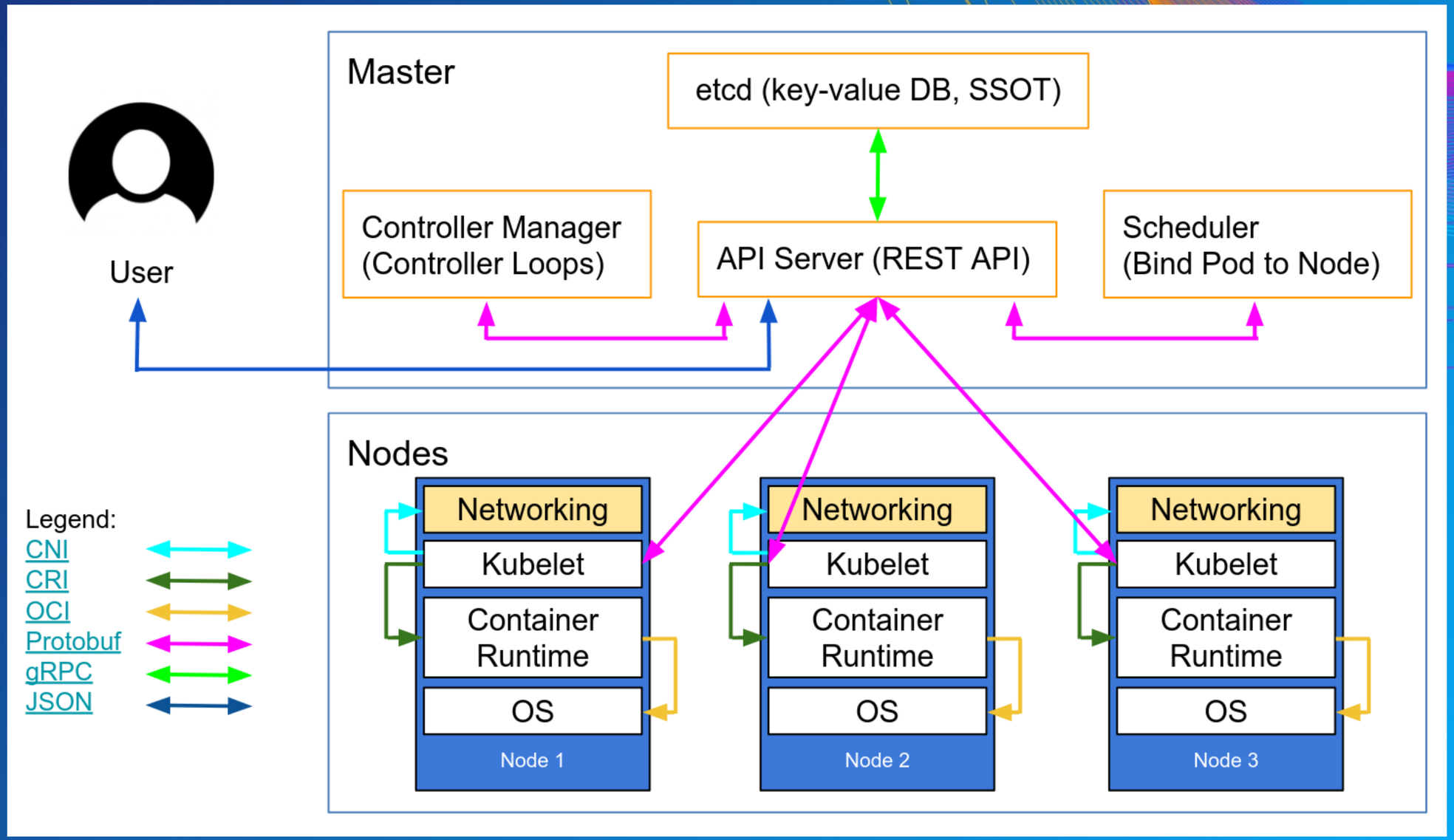
攻擊者驅動資安
Adversary Driven Security
Kubernetes 與 Container Runtime 之威脅建模
Threat Modeling of Kubernetes & Container Runtime
容器化的 MITRE ATT&CK 矩陣
MITRE ATT&CK Matrix for Containers
攻擊情境案例研究：弱點與濫用
Cases Study: Exploitable Vulnerabilities & Abuse the Legitimate Objects
稽核驅動資安
Audit Driven Security
理解CIS Kubernetes與Docker的評測基準
Outlines of the CIS Benchmarks with Kubernetes & Docker
CIS評測: 稽核缺失即錯誤設定
CIS Benchmarks: Audit Deficiencies as Misconfigurations
攻擊情境案例研究：錯誤設定
Cases Study: The Exploit to the Misconfigurations
防禦 Kubernetes
Defending Kubetnetes
使用MITRE D3FEND矩陣將最佳實踐與控制措施加以分類
Mapping the Best Practices & Controls to MITRE D3FEND Matrix



Ref: Kubernetes Components – Kubernetes.io

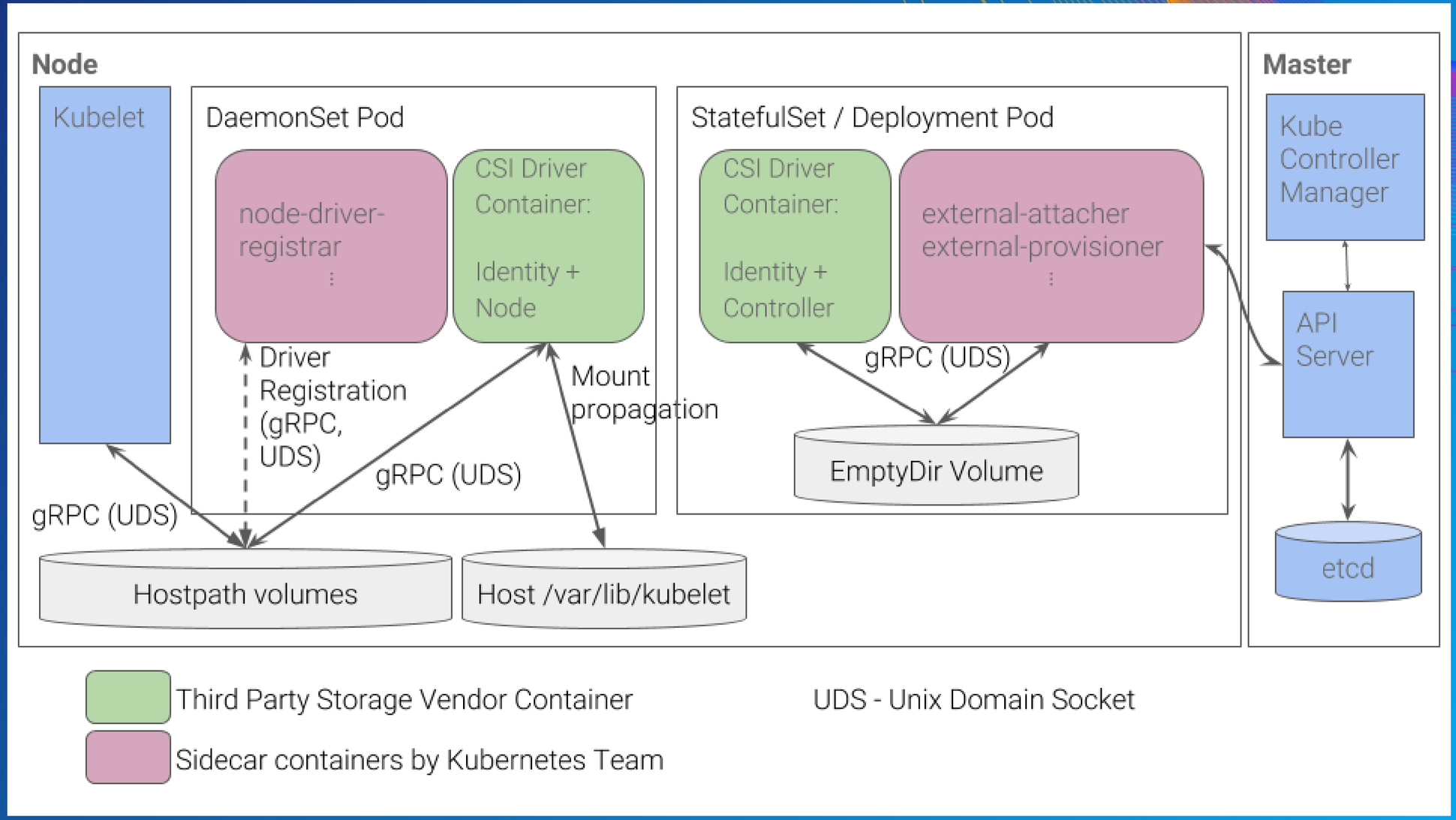
攻擊者驅動資安
Adversary Driven Security
Kubernetes 與 Container Runtime 之威脅建模
Threat Modeling of Kubernetes & Container Runtime
容器化的 MITRE ATT&CK 矩陣
MITRE ATT&CK Matrix for Containers
攻擊情境案例研究：弱點與濫用
Cases Study: Exploitable Vulnerabilities & Abuse the Legitimate Objects
稽核驅動資安
Audit Driven Security
理解CIS Kubernetes與Docker的評測基準
Outlines of the CIS Benchmarks with Kubernetes & Docker
CIS評測: 稽核缺失即錯誤設定
CIS Benchmarks: Audit Deficiencies as Misconfigurations
攻擊情境案例研究：錯誤設定
Cases Study: The Exploit to the Misconfigurations
防禦 Kubernetes
Defending Kubetnetes
使用MITRE D3FEND矩陣 將最佳實踐與控制措施加以分類
Mapping the Best Practices & Controls to MITRE D3FEND Matrix

Kubernetes Interfaces



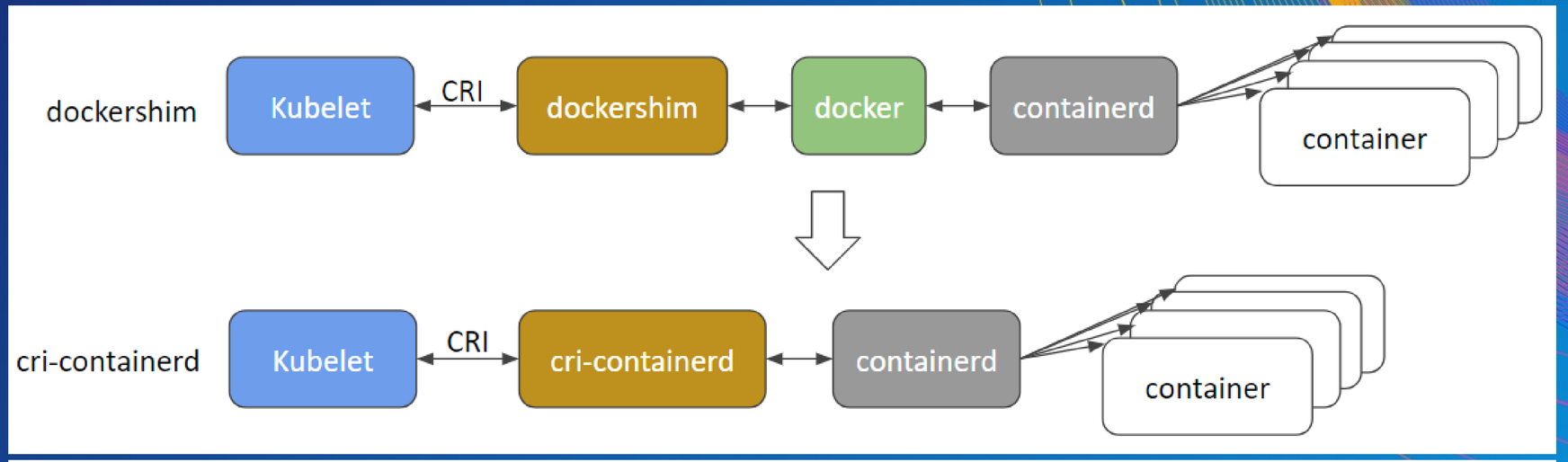
Ref: 11 Ways (Not) to Get Hacked – Kubernetes.io Blog by Andrew Martin

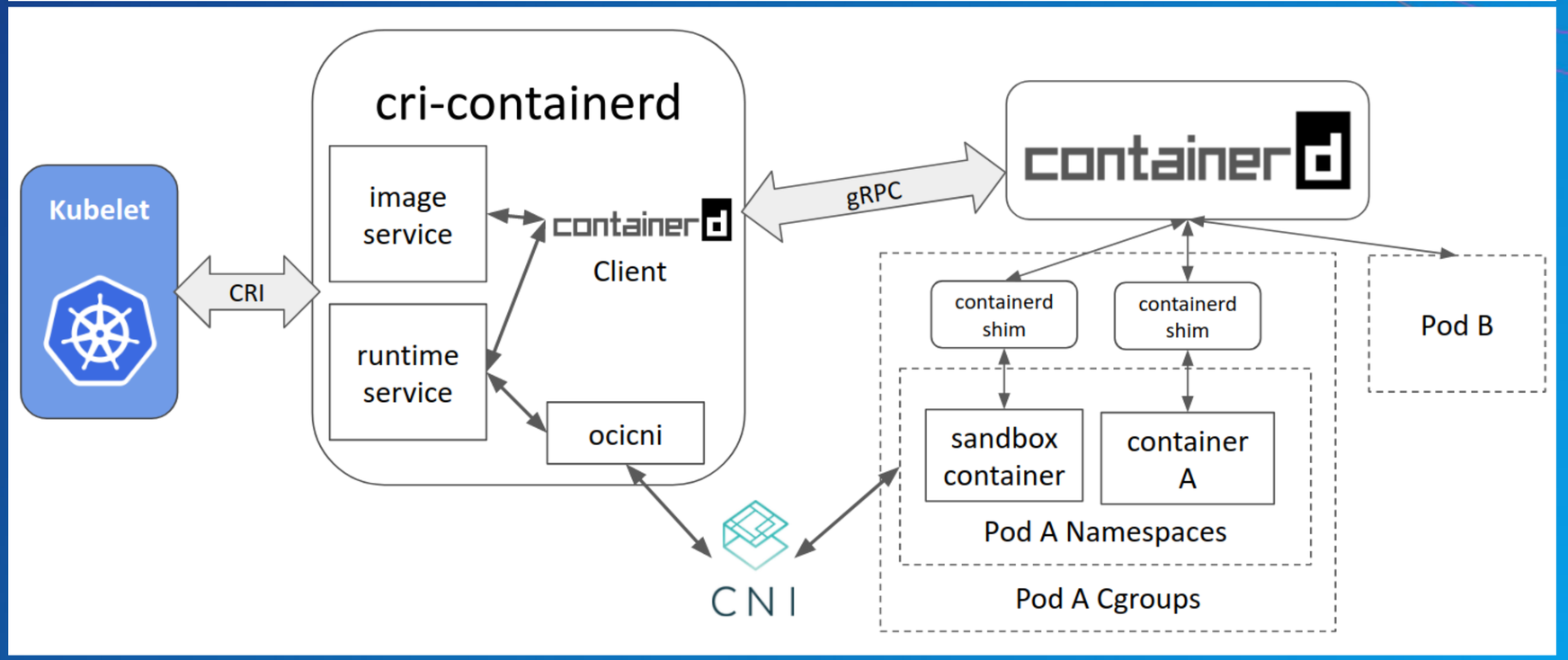
Kubernetes Interfaces



Ref: CSI Volume Plugins in Kubernetes Design Doc
– K8s Github, Design-Proposals-Archive

攻擊者驅動資安
Adversary Driven Security
Kubernetes 與 Container Runtime 之威脅建模
Threat Modeling of Kubernetes & Container Runtime
容器化的 MITRE ATT&CK 矩陣
MITRE ATT&CK Matrix for Containers
攻擊情境案例研究：弱點與濫用
Cases Study: Exploitable Vulnerabilities & Abuse the Legitimate Objects
稽核驅動資安
Audit Driven Security
理解CIS Kubernetes與Docker的評測基準
Outlines of the CIS Benchmarks with Kubernetes & Docker
CIS評測: 稽核缺失即錯誤設定
CIS Benchmarks: Audit Deficiencies as Misconfigurations
攻擊情境案例研究：錯誤設定
Cases Study: The Exploit to the Misconfigurations
防禦 Kubernetes
Defending Kubetnetes
使用MITRE D3FEND矩陣將最佳實踐與控制措施加以分類
Mapping the Best Practices & Controls to MITRE D3FEND Matrix





Ref: Containerd Brings More Container Runtime Options for Kubernetes – Kubernetes.io Blog by Antao Liu, Mike Brown

攻擊者驅動資安
Adversary Driven Security
Kubernetes 與 Container Runtime 之威脅建模
Threat Modeling of Kubernetes & Container Runtime
容器化的 MITRE ATT&CK 矩陣
MITRE ATT&CK Matrix for Containers
攻擊情境案例研究：弱點與濫用
Cases Study: Exploitable Vulnerabilities & Abuse the Legitimate Objects
稽核驅動資安
Audit Driven Security
理解CIS Kubernetes與Docker的評測基準
Outlines of the CIS Benchmarks with Kubernetes & Docker
CIS評測: 稽核缺失即錯誤設定
CIS Benchmarks: Audit Deficiencies as Misconfigurations
攻擊情境案例研究：錯誤設定
Cases Study: The Exploit to the Misconfigurations
防禦 Kubernetes
Defending Kubetnetes
使用MITRE D3FEND矩陣將最佳實踐與控制措施加以分類
Mapping the Best Practices & Controls to MITRE D3FEND Matrix

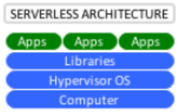
Distributed, Immutable, and Ephemeral (DIE)

CLOUD SECURITY Forum

The DIE Triad

BLOCKCHAIN

docker



Distributed (分散式)

DDoS resistant
分佈式拒絕服務抵抗

Availability

Immutable (不可改變的)

Easier Change Detection
變化更容易檢測和逆轉

Integrity

Ephemeral (短暫的)

Lower asset value for attackers
使資產價值接近於零

Confidentiality

@sounilyu ©

CYBERSEC 2023 臺灣資安大會 | 10

Ref: From CIA to DIE – by Sounil Yu @ CYBERSEC 2023

攻擊者驅動資安
Adversary Driven Security
Kubernetes 與 Container Runtime 之威脅建模
Threat Modeling of Kubernetes & Container Runtime
容器化的 MITRE ATT&CK 矩陣
MITRE ATT&CK Matrix for Containers
攻擊情境案例研究：弱點與濫用
Cases Study: Exploitable Vulnerabilities & Abuse the Legitimate Objects
稽核驅動資安
Audit Driven Security
理解CIS Kubernetes與Docker的評測基準
Outlines of the CIS Benchmarks with Kubernetes & Docker
CIS評測: 稽核缺失即錯誤設定
CIS Benchmarks: Audit Deficiencies as Misconfigurations
攻擊情境案例研究：錯誤設定
Cases Study: The Exploit to the Misconfigurations
防禦 Kubernetes
Defending Kubetnetes
使用MITRE D3FEND矩陣 將最佳實踐與控制措施加以分類
Mapping the Best Practices & Controls to MITRE D3FEND Matrix

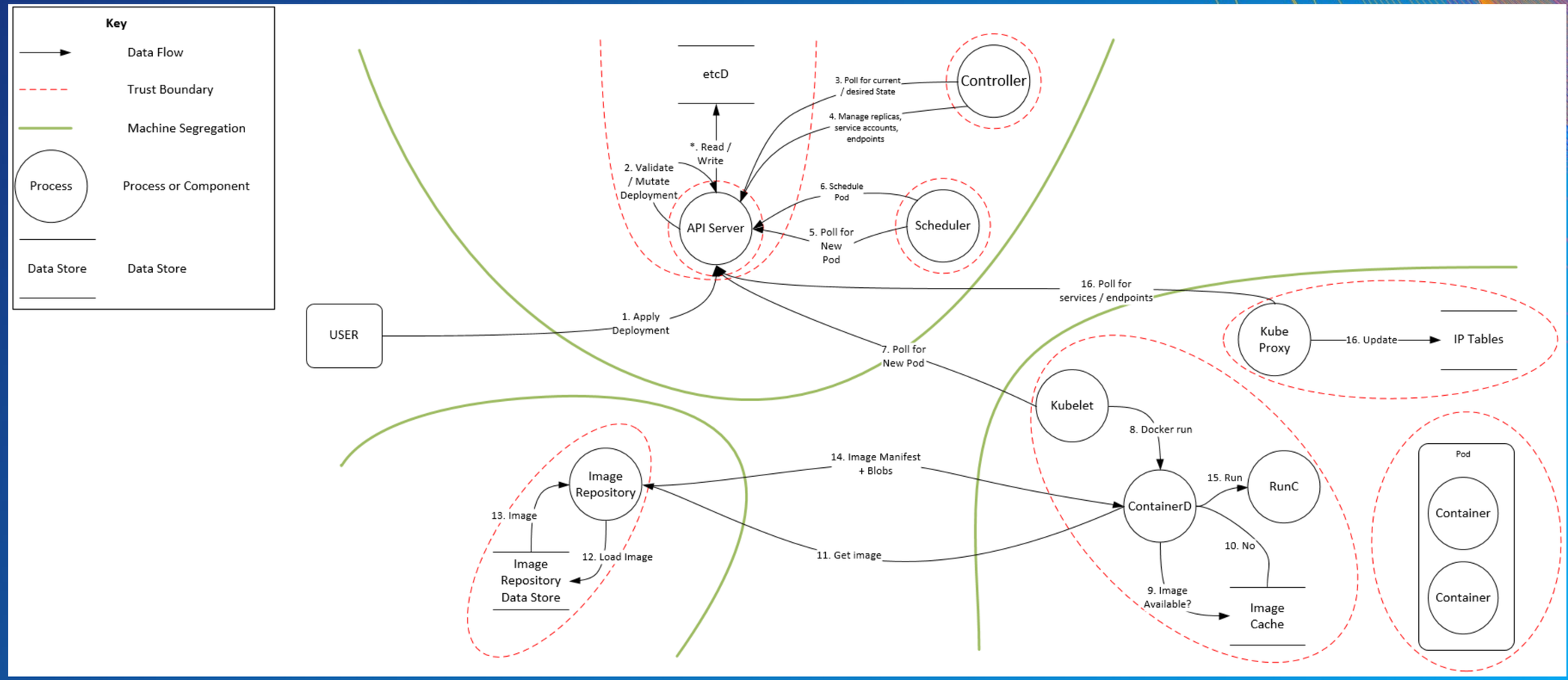
STRIDE with Distributed, Immutable, and Ephemeral (DIE)

CLOUD SECURITY Forum

STRIDE	DIE+ANA	CIA+ANA
Spoofing [欺騙]	Authentication [身分認證]	Authentication [認證]
Tampering [篡改]	Immutable [不可變]	Integrity [完整性]
Repudiation [否認]	Non-Repidiation (with Audit Logging) [不可否認性(稽核日誌)]	Non-Repidiation [不可否認性]
Information Disclosure [資訊洩露]	Ephemeral [短暫]	Confidentiality [機密性]
Denial of Service (DoS) [阻斷服務]	Distributed [分散式]	Availability [可用性]
Elevation of Privilege [權限提升]	Authorization [授權(帳號權限)]	Authorization [授權]

攻擊者驅動資安
Adversary Driven Security
Kubernetes 與 Container Runtime 之威脅建模
Threat Modeling of Kubernetes & Container Runtime
容器化的 MITRE ATT&CK 矩陣
MITRE ATT&CK Matrix for Containers
攻擊情境案例研究：弱點與濫用
Cases Study: Exploitable Vulnerabilities & Abuse the Legitimate Objects
稽核驅動資安
Audit Driven Security
理解CIS Kubernetes與Docker的評測基準
Outlines of the CIS Benchmarks with Kubernetes & Docker
CIS評測: 稽核缺失即錯誤設定
CIS Benchmarks: Audit Deficiencies as Misconfigurations
攻擊情境案例研究：錯誤設定
Cases Study: The Exploit to the Misconfigurations
防禦 Kubernetes
Defending Kubetnetes
使用MITRE D3FEND矩陣 將最佳實踐與控制措施加以分類
Mapping the Best Practices & Controls to MITRE D3FEND Matrix

Dataflow & Trust Boundaries Threat Modeling



Ref: K8s Attack Tree - Summary
– CNCF GitHub, financial-user-group: k8s-threat-model

攻擊者驅動資安
Adversary Driven Security
Kubernetes 與 Container Runtime 之威脅建模
Threat Modeling of Kubernetes & Container Runtime
容器化的 MITRE ATT&CK 矩陣
MITRE ATT&CK Matrix for Containers
攻擊情境案例研究：弱點與濫用
Cases Study: Exploitable Vulnerabilities & Abuse the Legitimate Objects
稽核驅動資安
Audit Driven Security
理解CIS Kubernetes與Docker的評測基準
Outlines of the CIS Benchmarks with Kubernetes & Docker
CIS評測: 稽核缺失即錯誤設定
CIS Benchmarks: Audit Deficiencies as Misconfigurations
攻擊情境案例研究：錯誤設定
Cases Study: The Exploit to the Misconfigurations
防禦 Kubernetes
Defending Kubetnetes
使用MITRE D3FEND矩陣將最佳實踐與控制措施加以分類
Mapping the Best Practices & Controls to MITRE D3FEND Matrix

Most Common Risks: OSWASP Kubernetes Top 10 - 2022

Risk (風險)	Summary (摘要)
K01: Insecure Workload Configurations (不安全的工作負載配置)	Workloads with overly permissive configurations (like running as root, privileged containers) can lead to compromise.
K02: Supply Chain Vulnerabilities (供應鏈漏洞)	Vulnerabilities in container images and dependencies can be exploited if not properly managed.
K03: Overly Permissive RBAC Configurations (過度寬鬆的 RBAC 設定值)	Misconfigured Role-Based Access Control can grant excessive permissions, leading to privilege escalation.
K04: Lack of Centralized Policy Enforcement (缺乏集中化策略執行)	Lack of consistent policy enforcement across clusters can lead to misconfigurations and security gaps.
K05: Inadequate Logging and Monitoring (不足的日誌記錄和監控)	Insufficient logging and monitoring hinder detection and response to security incidents.

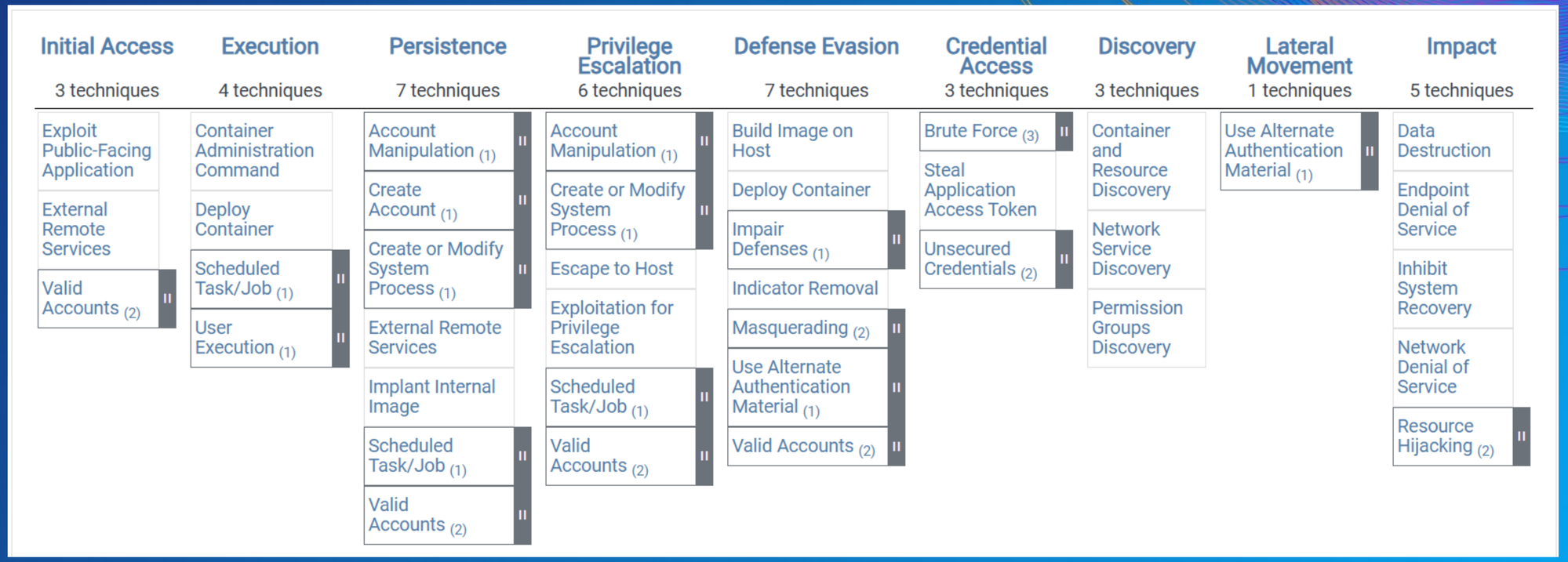
攻擊者驅動資安
Adversary Driven Security
Kubernetes 與 Container Runtime 之威脅建模
Threat Modeling of Kubernetes & Container Runtime
容器化的 MITRE ATT&CK 矩陣
MITRE ATT&CK Matrix for Containers
攻擊情境案例研究：弱點與濫用
Cases Study: Exploitable Vulnerabilities & Abuse the Legitimate Objects
稽核驅動資安
Audit Driven Security
理解CIS Kubernetes與Docker的評測基準
Outlines of the CIS Benchmarks with Kubernetes & Docker
CIS評測: 稽核缺失即錯誤設定
CIS Benchmarks: Audit Deficiencies as Misconfigurations
攻擊情境案例研究：錯誤設定
Cases Study: The Exploit to the Misconfigurations
防禦 Kubernetes
Defending Kubetnetes
使用MITRE D3FEND矩陣 將最佳實踐與控制措施加以分類
Mapping the Best Practices & Controls to MITRE D3FEND Matrix

Most Common Risks: OSWASP Kubernetes Top 10 - 2022

Risk (風險)	Summary (摘要)
K06: Broken Authentication Mechanisms (身份驗證機制失效)	Weak or improperly configured authentication mechanisms can allow unauthorized access to the cluster API.
K07: Missing Network Segmentation Controls (缺少網路分段控制措施)	Lack of network segmentation allows compromised workloads to easily move laterally within the cluster.
K08: Secrets Management Failures (機密管理失效)	Improper storage and handling of secrets can lead to their exposure.
K09: Misconfigured Cluster Components (錯誤設定的叢集組成元件)	Misconfigurations in core Kubernetes components (like kubelet, etcd, kube-apiserver) can lead to compromise.
K10: Outdated and Vulnerable Kubernetes Components (過時且有漏洞的 Kubernetes 組成元件)	Unpatched vulnerabilities in Kubernetes and its components can be exploited by attackers.

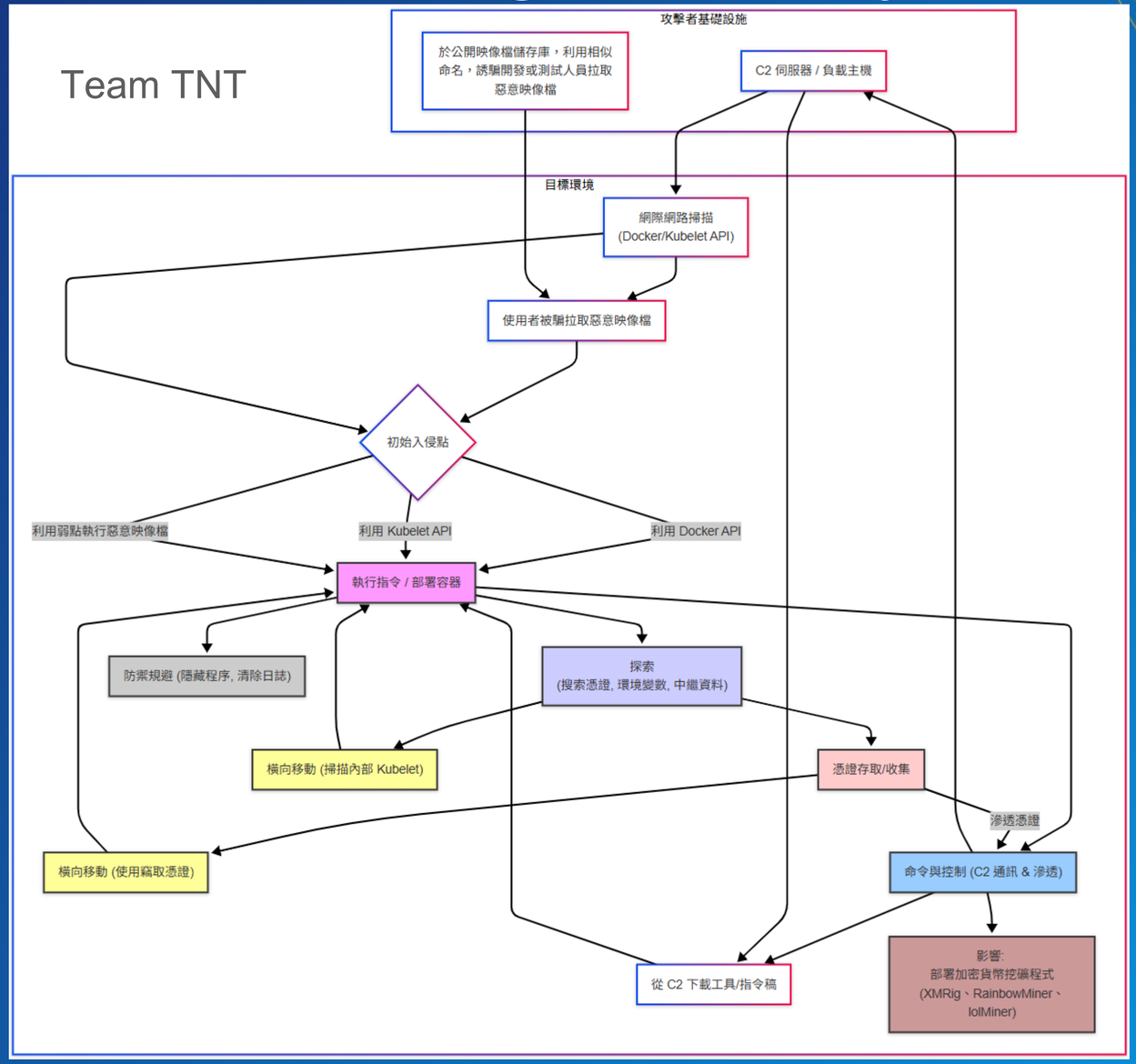
攻擊者驅動資安
Adversary Driven Security
Kubernetes 與 Container Runtime 之威脅建模
Threat Modeling of Kubernetes & Container Runtime
容器化的 MITRE ATT&CK 矩陣
MITRE ATT&CK Matrix for Containers
攻擊情境案例研究：弱點與濫用
Cases Study: Exploitable Vulnerabilities & Abuse the Legitimate Objects
稽核驅動資安
Audit Driven Security
理解CIS Kubernetes與Docker的評測基準
Outlines of the CIS Benchmarks with Kubernetes & Docker
CIS評測: 稽核缺失即錯誤設定
CIS Benchmarks: Audit Deficiencies as Misconfigurations
攻擊情境案例研究：錯誤設定
Cases Study: The Exploit to the Misconfigurations
防禦 Kubernetes
Defending Kubetnetes
使用MITRE D3FEND矩陣 將最佳實踐與控制措施加以分類
Mapping the Best Practices & Controls to MITRE D3FEND Matrix

MITRE ATT&CK Matrix for Containers



攻擊者驅動資安
Adversary Driven Security
Kubernetes 與 Container Runtime 之威脅建模
Threat Modeling of Kubernetes & Container Runtime
容器化的 MITRE ATT&CK 矩陣
MITRE ATT&CK Matrix for Containers
攻擊情境案例研究：弱點與濫用
Cases Study: Exploitable Vulnerabilities & Abuse the Legitimate Objects
稽核驅動資安
Audit Driven Security
理解CIS Kubernetes與Docker的評測基準
Outlines of the CIS Benchmarks with Kubernetes & Docker
CIS評測: 稽核缺失即錯誤設定
CIS Benchmarks: Audit Deficiencies as Misconfigurations
攻擊情境案例研究：錯誤設定
Cases Study: The Exploit to the Misconfigurations
防禦 Kubernetes
Defending Kubetnetes
使用MITRE D3FEND矩陣 將最佳實踐與控制措施加以分類
Mapping the Best Practices & Controls to MITRE D3FEND Matrix

Cases Study: Exploitable Vulnerabilities & Abuse the Legitimate Objects

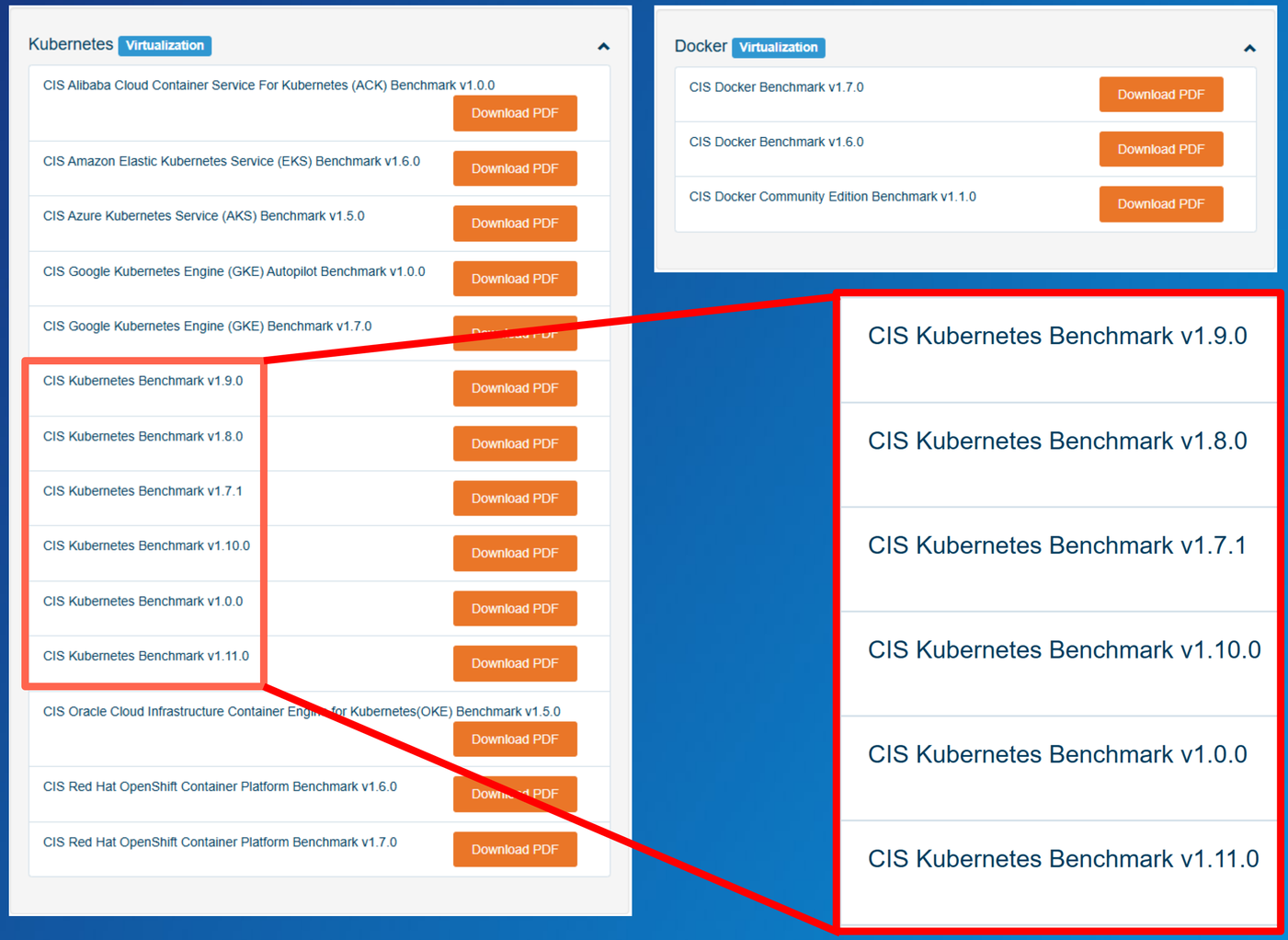


CYBERSEC 2025
臺灣資安大會

Audit Driven Security (稽核驅動資安)

攻擊者驅動資安
Adversary Driven Security
Kubernetes 與 Container Runtime 之威脅建模
Threat Modeling of Kubernetes & Container Runtime
容器化的 MITRE ATT&CK 矩陣
MITRE ATT&CK Matrix for Containers
攻擊情境案例研究：弱點與濫用
Cases Study: Exploitable Vulnerabilities & Abuse the Legitimate Objects
稽核驅動資安
Audit Driven Security
理解CIS Kubernetes與Docker的評測基準
Outlines of the CIS Benchmarks with Kubernetes & Docker
CIS評測: 稽核缺失即錯誤設定
CIS Benchmarks: Audit Deficiencies as Misconfigurations
攻擊情境案例研究：錯誤設定
Cases Study: The Exploit to the Misconfigurations
防禦 Kubernetes
Defending Kubetnetes
使用MITRE D3FEND矩陣將最佳實踐與控制措施加以分類
Mapping the Best Practices & Controls to MITRE D3FEND Matrix

Outlines of the CIS Benchmarks with Kubernetes & Docker



https://downloads.cisecurity.org/

攻擊者驅動資安
Adversary Driven Security
Kubernetes 與 Container Runtime 之威脅建模
Threat Modeling of Kubernetes & Container Runtime
容器化的 MITRE ATT&CK 矩陣
MITRE ATT&CK Matrix for Containers
攻擊情境案例研究：弱點與濫用
Cases Study: Exploitable Vulnerabilities & Abuse the Legitimate Objects
稽核驅動資安
Audit Driven Security
理解CIS Kubernetes與Docker的評測基準
Outlines of the CIS Benchmarks with Kubernetes & Docker
CIS評測: 稽核缺失即錯誤設定
CIS Benchmarks: Audit Deficiencies as Misconfigurations
攻擊情境案例研究：錯誤設定
Cases Study: The Exploit to the Misconfigurations
防禦 Kubernetes
Defending Kubetnetes
使用MITRE D3FEND矩陣 將最佳實踐與控制措施加以分類
Mapping the Best Practices & Controls to MITRE D3FEND Matrix

Key Concepts of Recommendation

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted, or the component will not be included in the recommendation.

Title

Concise description for the recommendation's intended configuration.

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile

A collection of recommendations for securing a technology or a supporting platform. Most benchmarks include at least a Level 1 and Level 2 Profile. Level 2 extends Level 1 recommendations and is not a standalone profile. The Profile Definitions section in the benchmark provides the definitions as they pertain to the recommendations included for the technology.

Description

Detailed information pertaining to the setting with which the recommendation is concerned. In some cases, the description will include the recommended value.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Impact Statement

Any security, functionality, or operational consequences that can result from following the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation.

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Default Value

Default value for the given setting in this recommendation, if known. If not known, either not configured or not defined will be applied.

References

Additional documentation relative to the recommendation.

CIS Critical Security Controls® (CIS Controls®)

The mapping between a recommendation and the CIS Controls is organized by CIS Controls version, Safeguard, and Implementation Group (IG). The Benchmark in its entirety addresses the CIS Controls safeguards of (v7) “5.1 - Establish Secure Configurations” and (v8) '4.1 - Establish and Maintain a Secure Configuration Process” so individual recommendations will not be mapped to these safeguards.

Additional Information

Supplementary information that does not correspond to any other field but may be useful to the user.

攻擊者驅動資安
Adversary Driven Security
Kubernetes 與 Container Runtime 之威脅建模
Threat Modeling of Kubernetes & Container Runtime
容器化的 MITRE ATT&CK 矩陣
MITRE ATT&CK Matrix for Containers
攻擊情境案例研究：弱點與濫用
Cases Study: Exploitable Vulnerabilities & Abuse the Legitimate Objects
稽核驅動資安
Audit Driven Security
理解CIS Kubernetes與Docker的評測基準
Outlines of the CIS Benchmarks with Kubernetes & Docker
CIS評測: 稽核缺失即錯誤設定
CIS Benchmarks: Audit Deficiencies as Misconfigurations
攻擊情境案例研究：錯誤設定
Cases Study: The Exploit to the Misconfigurations
防禦 Kubernetes
Defending Kubetnetes
使用MITRE D3FEND矩陣 將最佳實踐與控制措施加以分類
Mapping the Best Practices & Controls to MITRE D3FEND Matrix

Profile Levels

Feature	CIS Level 1	CIS Level 2
Security Goal	Foundational security, lower attack surface, basic hygiene	Defense in depth, higher security for paramount environments
Implementation	Easier, quicker, less expertise needed	More complex, time-consuming, requires significant expertise and testing
Operational Impact	Minimal expected impact on performance/functionality	Potential adverse effects if not implemented with due care; requires careful validation
Target Environment	General purpose, baseline for most organizations	High-security environments, sensitive data, critical systems, regulated industries
Typical Scope (K8s)	Practical, prudent settings, clear security benefit, minimal utility impact	More stringent configurations, potentially impacting usability or performance, deeper security controls

攻擊者驅動資安
Adversary Driven Security
Kubernetes 與 Container Runtime 之威脅建模
Threat Modeling of Kubernetes & Container Runtime
容器化的 MITRE ATT&CK 矩陣
MITRE ATT&CK Matrix for Containers
攻擊情境案例研究：弱點與濫用
Cases Study: Exploitable Vulnerabilities & Abuse the Legitimate Objects
稽核驅動資安
Audit Driven Security
理解CIS Kubernetes與Docker的評測基準
Outlines of the CIS Benchmarks with Kubernetes & Docker
CIS評測: 稽核缺失即錯誤設定
CIS Benchmarks: Audit Deficiencies as Misconfigurations
攻擊情境案例研究：錯誤設定
Cases Study: The Exploit to the Misconfigurations
防禦 Kubernetes
Defending Kubetnetes
使用MITRE D3FEND矩陣 將最佳實踐與控制措施加以分類
Mapping the Best Practices & Controls to MITRE D3FEND Matrix

Outlines of the CIS Benchmarks with Kubernetes & Docker

Benchmark	Category	Scope of Checks
Kubernetes	**Control Plane Components**	Configuration files and runtime settings for kube-apiserver, kube-controller-manager, kube-scheduler, and control plane node configurations.
Kubernetes	**etcd**	Security configuration of the etcd datastore, including authentication, encryption, and access control.
Kubernetes	**Control Plane Configuration**	Cluster-wide configuration aspects like authentication, authorization (RBAC), and audit logging.
Kubernetes	**Worker Nodes**	Configuration files and runtime settings for kubelet and kube-proxy on worker nodes.
Kubernetes	**Policies**	Cluster-wide security policies related to RBAC, network segmentation, pod security, secrets management, and resource limits.
Docker	**Container Runtime Configuration** (Req. 5.1~5.32)	Container Runtime process parameters and configurations.

攻擊者驅動資安
Adversary Driven Security
Kubernetes 與 Container Runtime 之威脅建模
Threat Modeling of Kubernetes & Container Runtime
容器化的 MITRE ATT&CK 矩陣
MITRE ATT&CK Matrix for Containers
攻擊情境案例研究：弱點與濫用
Cases Study: Exploitable Vulnerabilities & Abuse the Legitimate Objects
稽核驅動資安
Audit Driven Security
理解CIS Kubernetes與Docker的評測基準
Outlines of the CIS Benchmarks with Kubernetes & Docker
CIS評測: 稽核缺失即錯誤設定
CIS Benchmarks: Audit Deficiencies as Misconfigurations
攻擊情境案例研究：錯誤設定
Cases Study: The Exploit to the Misconfigurations
防禦 Kubernetes
Defending Kubetnetes
使用MITRE D3FEND矩陣 將最佳實踐與控制措施加以分類
Mapping the Best Practices & Controls to MITRE D3FEND Matrix

CIS Kubernetes Benchmark Compatibility

Kubernetes Benchmarks	Kubernetes versions
CIS 1.7.1	1.25
CIS 1.8	1.26
CIS 1.9	1.27-1.29
CIS 1.10	1.28-1.31
CIS 1.11	1.29-1.32

攻擊者驅動資安
Adversary Driven Security
Kubernetes 與 Container Runtime 之威脅建模
Threat Modeling of Kubernetes & Container Runtime
容器化的 MITRE ATT&CK 矩陣
MITRE ATT&CK Matrix for Containers
攻擊情境案例研究：弱點與濫用
Cases Study: Exploitable Vulnerabilities & Abuse the Legitimate Objects
稽核驅動資安
Audit Driven Security
理解CIS Kubernetes與Docker的評測基準
Outlines of the CIS Benchmarks with Kubernetes & Docker
CIS評測: 稽核缺失即錯誤設定
CIS Benchmarks: Audit Deficiencies as Misconfigurations
攻擊情境案例研究：錯誤設定
Cases Study: The Exploit to the Misconfigurations
防禦 Kubernetes
Defending Kubetnetes
使用MITRE D3FEND矩陣將最佳實踐與控制措施加以分類
Mapping the Best Practices & Controls to MITRE D3FEND Matrix

Control Plane Components: Control Plane Node Configuration Files

- 21 Level 1 Profile Checks, 0 Level 2 Profile Checks:

Audits verify the ownership and permissions of critical configuration files, such as the admin config files (/etc/kubernetes/admin.conf), PKI certificates and keys, CNI files, and the manifest files used by the kubelet to run static pods for control plane components.

- Audit Deficiencies Implication:

Incorrect permissions (e.g., world-readable private keys) could lead to credential theft, or unauthorized modification of control plane configurations.

攻擊者驅動資安
Adversary Driven Security
Kubernetes 與 Container Runtime 之威脅建模
Threat Modeling of Kubernetes & Container Runtime
容器化的 MITRE ATT&CK 矩陣
MITRE ATT&CK Matrix for Containers
攻擊情境案例研究：弱點與濫用
Cases Study: Exploitable Vulnerabilities & Abuse the Legitimate Objects
稽核驅動資安
Audit Driven Security
理解CIS Kubernetes與Docker的評測基準
Outlines of the CIS Benchmarks with Kubernetes & Docker
CIS評測: 稽核缺失即錯誤設定
CIS Benchmarks: Audit Deficiencies as Misconfigurations
攻擊情境案例研究：錯誤設定
Cases Study: The Exploit to the Misconfigurations
防禦 Kubernetes
Defending Kubetnetes
使用MITRE D3FEND矩陣將最佳實踐與控制措施加以分類
Mapping the Best Practices & Controls to MITRE D3FEND Matrix

Control Plane Components: API Server

- 27 Level 1 Profile Checks, 3 Level 2 Profile Checks:

The recommendations enhance API server security by enforcing strict authentication, authorization, and secure communication protocols. They ensure proper TLS and certificate configurations between cluster components while limiting potentially risky behaviors through tailored admission controllers. Comprehensive logging, auditing, and encryption practices further protect sensitive data and help maintain a robust, resilient Kubernetes control plane.

- Audit Deficiencies Implication:

Failing on these checks indicates critical security gaps, such as allowing unauthenticated access, lacking proper authorization, permitting insecure pods, or failing to log security events, directly enabling TTPs like "External Remote Services (T1133)" or "Privilege Escalation" via RBAC bypass.

攻擊者驅動資安
Adversary Driven Security
Kubernetes 與 Container Runtime 之威脅建模
Threat Modeling of Kubernetes & Container Runtime
容器化的 MITRE ATT&CK 矩陣
MITRE ATT&CK Matrix for Containers
攻擊情境案例研究：弱點與濫用
Cases Study: Exploitable Vulnerabilities & Abuse the Legitimate Objects
稽核驅動資安
Audit Driven Security
理解CIS Kubernetes與Docker的評測基準
Outlines of the CIS Benchmarks with Kubernetes & Docker
CIS評測: 稽核缺失即錯誤設定
CIS Benchmarks: Audit Deficiencies as Misconfigurations
攻擊情境案例研究：錯誤設定
Cases Study: The Exploit to the Misconfigurations
防禦 Kubernetes
Defending Kubetnetes
使用MITRE D3FEND矩陣將最佳實踐與控制措施加以分類
Mapping the Best Practices & Controls to MITRE D3FEND Matrix

Control Plane Components: Controller Manager

- 7 Level 1 Profile Checks, 0 Level 2 Profile Checks:

Audits focus on arguments like ensuring it uses its dedicated service account credentials (--use-service-account-credentials=true), disabling profiling (--profiling=false), and binding to a secure address.

- Audit Deficiencies Implication:

Misconfigurations might allow unauthorized actions if the controller manager's identity is compromised or expose performance data.

攻擊者驅動資安
Adversary Driven Security
Kubernetes 與 Container Runtime 之威脅建模
Threat Modeling of Kubernetes & Container Runtime
容器化的 MITRE ATT&CK 矩陣
MITRE ATT&CK Matrix for Containers
攻擊情境案例研究：弱點與濫用
Cases Study: Exploitable Vulnerabilities & Abuse the Legitimate Objects
稽核驅動資安
Audit Driven Security
理解CIS Kubernetes與Docker的評測基準
Outlines of the CIS Benchmarks with Kubernetes & Docker
CIS評測: 稽核缺失即錯誤設定
CIS Benchmarks: Audit Deficiencies as Misconfigurations
攻擊情境案例研究：錯誤設定
Cases Study: The Exploit to the Misconfigurations
防禦 Kubernetes
Defending Kubetnetes
使用MITRE D3FEND矩陣將最佳實踐與控制措施加以分類
Mapping the Best Practices & Controls to MITRE D3FEND Matrix

Control Plane Components: Scheduler

- 2 Level 1 Profile Checks, 0 Level 2 Profile Checks:

Similar to the controller manager, checks focus on disabling profiling and binding to a secure address.

- Audit Deficiencies Implication:

Exposes performance data or allows potential unauthorized interaction with the scheduler.

攻擊者驅動資安
Adversary Driven Security
Kubernetes 與 Container Runtime 之威脅建模
Threat Modeling of Kubernetes & Container Runtime
容器化的 MITRE ATT&CK 矩陣
MITRE ATT&CK Matrix for Containers
攻擊情境案例研究：弱點與濫用
Cases Study: Exploitable Vulnerabilities & Abuse the Legitimate Objects
稽核驅動資安
Audit Driven Security
理解CIS Kubernetes與Docker的評測基準
Outlines of the CIS Benchmarks with Kubernetes & Docker
CIS評測: 稽核缺失即錯誤設定
CIS Benchmarks: Audit Deficiencies as Misconfigurations
攻擊情境案例研究：錯誤設定
Cases Study: The Exploit to the Misconfigurations
防禦 Kubernetes
Defending Kubetnetes
使用MITRE D3FEND矩陣 將最佳實踐與控制措施加以分類
Mapping the Best Practices & Controls to MITRE D3FEND Matrix

etcd

- 7 Level 1 Profile Checks, 1 Level 2 Profile Checks:

The etcd audit contents primarily aims to secure the etcd service. This involves ensuring that all client and peer communication is encrypted using TLS, enforcing client authentication to prevent unauthorized access, and disabling auto-TLS to avoid reliance on self-signed certificates. Additionally, it mandates the use of a unique Certificate Authority (CA) for etcd, separate from the Kubernetes cluster's CA, to further restrict access.

- Audit Deficiencies Implication:

Exposed or unencrypted etcd allows attackers direct access to all cluster secrets, configurations, and state, leading to complete cluster compromise.

攻擊者驅動資安

Adversary Driven Security

Kubernetes 與 Container Runtime 之威脅建模

Threat Modeling of Kubernetes & Container Runtime

容器化的 MITRE ATT&CK 矩陣

MITRE ATT&CK Matrix for Containers

攻擊情境案例研究：弱點與濫用

Cases Study: Exploitable Vulnerabilities & Abuse the Legitimate Objects

稽核驅動資安

Audit Driven Security

理解CIS Kubernetes與Docker的評測基準

Outlines of the CIS Benchmarks with Kubernetes & Docker

CIS評測: 稽核缺失即錯誤設定

CIS Benchmarks: Audit Deficiencies as Misconfigurations

攻擊情境案例研究：錯誤設定

Cases Study: The Exploit to the Misconfigurations

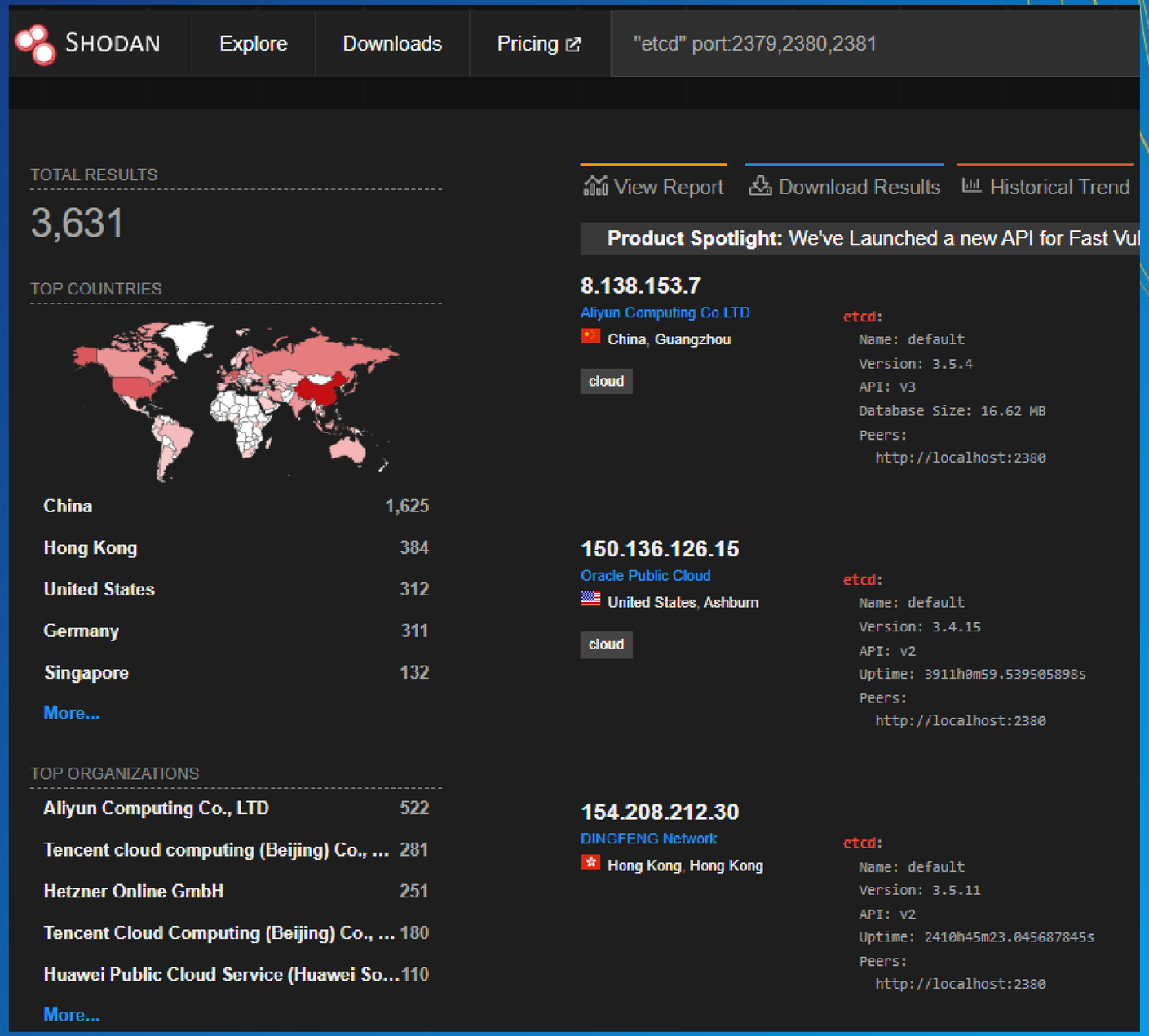
防禦 Kubernetes

Defending Kubetnetes

使用MITRE D3FEND矩陣 將最佳實踐與控制措施加以分類

Mapping the Best Practices & Controls to MITRE D3FEND Matrix

etcd



攻擊者驅動資安
Adversary Driven Security
Kubernetes 與 Container Runtime 之威脅建模
Threat Modeling of Kubernetes & Container Runtime
容器化的 MITRE ATT&CK 矩陣
MITRE ATT&CK Matrix for Containers
攻擊情境案例研究：弱點與濫用
Cases Study: Exploitable Vulnerabilities & Abuse the Legitimate Objects
稽核驅動資安
Audit Driven Security
理解CIS Kubernetes與Docker的評測基準
Outlines of the CIS Benchmarks with Kubernetes & Docker
CIS評測: 稽核缺失即錯誤設定
CIS Benchmarks: Audit Deficiencies as Misconfigurations
攻擊情境案例研究：錯誤設定
Cases Study: The Exploit to the Misconfigurations
防禦 Kubernetes
Defending Kubetnetes
使用MITRE D3FEND矩陣將最佳實踐與控制措施加以分類
Mapping the Best Practices & Controls to MITRE D3FEND Matrix

Control Plane Configuration: Authentication and Authorization

- 3 Level 1 Profile Checks, 0 Level 2 Profile Checks:

Audits re-verify that strong authentication is enforced (no anonymous access) and that RBAC is the primary authorization mode, configured following the principle of least privilege.

- Audit Deficiencies Implication:

Weak authentication or authorization allows unauthorized access and actions within the cluster.

攻擊者驅動資安
Adversary Driven Security
Kubernetes 與 Container Runtime 之威脅建模
Threat Modeling of Kubernetes & Container Runtime
容器化的 MITRE ATT&CK 矩陣
MITRE ATT&CK Matrix for Containers
攻擊情境案例研究：弱點與濫用
Cases Study: Exploitable Vulnerabilities & Abuse the Legitimate Objects
稽核驅動資安
Audit Driven Security
理解CIS Kubernetes與Docker的評測基準
Outlines of the CIS Benchmarks with Kubernetes & Docker
CIS評測: 稽核缺失即錯誤設定
CIS Benchmarks: Audit Deficiencies as Misconfigurations
攻擊情境案例研究：錯誤設定
Cases Study: The Exploit to the Misconfigurations
防禦 Kubernetes
Defending Kubetnetes
使用MITRE D3FEND矩陣將最佳實踐與控制措施加以分類
Mapping the Best Practices & Controls to MITRE D3FEND Matrix

Control Plane Configuration: Logging

- 1 Level 1 Profile Checks, 1 Level 2 Profile Checks:

Audits ensure Kubernetes audit logging is enabled, configured with an appropriate policy to capture meaningful events (metadata, request, response stages), and logs are sent to a persistent, secure location, with appropriate retention policies.

- Audit Deficiencies Implication:

Lack of audit logs severely hinders detection, investigation, and response to security incidents.

攻擊者驅動資安
Adversary Driven Security
Kubernetes 與 Container Runtime 之威脅建模
Threat Modeling of Kubernetes & Container Runtime
容器化的 MITRE ATT&CK 矩陣
MITRE ATT&CK Matrix for Containers
攻擊情境案例研究：弱點與濫用
Cases Study: Exploitable Vulnerabilities & Abuse the Legitimate Objects
稽核驅動資安
Audit Driven Security
理解CIS Kubernetes與Docker的評測基準
Outlines of the CIS Benchmarks with Kubernetes & Docker
CIS評測: 稽核缺失即錯誤設定
CIS Benchmarks: Audit Deficiencies as Misconfigurations
攻擊情境案例研究：錯誤設定
Cases Study: The Exploit to the Misconfigurations
防禦 Kubernetes
Defending Kubetnetes
使用MITRE D3FEND矩陣將最佳實踐與控制措施加以分類
Mapping the Best Practices & Controls to MITRE D3FEND Matrix

Worker Nodes: Worker Node Configuration Files

- 10 Level 1 Profile Checks, 0 Level 2 Profile Checks:

Checks ensure proper ownership (root:root) and restrictive permissions (e.g., 600) for kubelet and kube-proxy configuration files and any associated certificate files.

- Audit Deficiencies Implication:

Allows unauthorized users on the node to read sensitive configurations or modify agent behavior.

攻擊者驅動資安
Adversary Driven Security
Kubernetes 與 Container Runtime 之威脅建模
Threat Modeling of Kubernetes & Container Runtime
容器化的 MITRE ATT&CK 矩陣
MITRE ATT&CK Matrix for Containers
攻擊情境案例研究：弱點與濫用
Cases Study: Exploitable Vulnerabilities & Abuse the Legitimate Objects
稽核驅動資安
Audit Driven Security
理解CIS Kubernetes與Docker的評測基準
Outlines of the CIS Benchmarks with Kubernetes & Docker
CIS評測: 稽核缺失即錯誤設定
CIS Benchmarks: Audit Deficiencies as Misconfigurations
攻擊情境案例研究：錯誤設定
Cases Study: The Exploit to the Misconfigurations
防禦 Kubernetes
Defending Kubetnetes
使用MITRE D3FEND矩陣將最佳實踐與控制措施加以分類
Mapping the Best Practices & Controls to MITRE D3FEND Matrix

Worker Nodes: Kubelet

- 13 Level 1 Profile Checks, 2 Level 2 Profile Checks:

The audit of Kubelet in Worker Nodes aims to enhance its security by focusing on authentication, authorization, communication security, and resource management. Implementing these recommendations helps reduce potential risks and improves the overall security posture of Kubernetes nodes. By ensuring proper configurations and utilizing security enhancements, organizations can create a more secure and reliable Kubernetes environment.

- Audit Deficiencies Implication:

An insecure Kubelet allows attackers to bypass API server controls, execute commands in pods on the node, retrieve logs, or potentially gain node-level access.

攻擊者驅動資安
Adversary Driven Security
Kubernetes 與 Container Runtime 之威脅建模
Threat Modeling of Kubernetes & Container Runtime
容器化的 MITRE ATT&CK 矩陣
MITRE ATT&CK Matrix for Containers
攻擊情境案例研究：弱點與濫用
Cases Study: Exploitable Vulnerabilities & Abuse the Legitimate Objects
稽核驅動資安
Audit Driven Security
理解CIS Kubernetes與Docker的評測基準
Outlines of the CIS Benchmarks with Kubernetes & Docker
CIS評測: 稽核缺失即錯誤設定
CIS Benchmarks: Audit Deficiencies as Misconfigurations
攻擊情境案例研究：錯誤設定
Cases Study: The Exploit to the Misconfigurations
防禦 Kubernetes
Defending Kubetnetes
使用MITRE D3FEND矩陣將最佳實踐與控制措施加以分類
Mapping the Best Practices & Controls to MITRE D3FEND Matrix

Worker Nodes: kube-proxy

- Only 1 Level 1 Profile Checks:

Audits check its configuration file settings and command-line arguments for secure defaults. Ensure that the --metrics-bind-address parameter is not set to a value other than 127.0.0.1. From the output of this command gather the location specified in the --config parameter. Review any file stored at that location and ensure that it does not specify a value other than 127.0.0.1 for metricsBindAddress.

- Audit Deficiencies Implication:

Misconfigured kube-proxy could potentially lead to network policy bypass or traffic manipulation.

攻擊者驅動資安
Adversary Driven Security
Kubernetes 與 Container Runtime 之威脅建模
Threat Modeling of Kubernetes & Container Runtime
容器化的 MITRE ATT&CK 矩陣
MITRE ATT&CK Matrix for Containers
攻擊情境案例研究：弱點與濫用
Cases Study: Exploitable Vulnerabilities & Abuse the Legitimate Objects
稽核驅動資安
Audit Driven Security
理解CIS Kubernetes與Docker的評測基準
Outlines of the CIS Benchmarks with Kubernetes & Docker
CIS評測: 稽核缺失即錯誤設定
CIS Benchmarks: Audit Deficiencies as Misconfigurations
攻擊情境案例研究：錯誤設定
Cases Study: The Exploit to the Misconfigurations
防禦 Kubernetes
Defending Kubetnetes
使用MITRE D3FEND矩陣將最佳實踐與控制措施加以分類
Mapping the Best Practices & Controls to MITRE D3FEND Matrix

Policies: RBAC and Service Accounts

- 12 Level 1 Profile Checks, 0 Level 2 Profile Checks:

Audits verify that Roles and ClusterRoles adhere to least privilege. Checks ensure cluster-admin access is minimized, default service accounts are not used or have minimal permissions, and service account token automounting is disabled where not needed (automountServiceAccountToken: false).

- Audit Deficiencies Implication:

Overly permissive RBAC is a primary vector for privilege escalation.

攻擊者驅動資安
Adversary Driven Security
Kubernetes 與 Container Runtime 之威脅建模
Threat Modeling of Kubernetes & Container Runtime
容器化的 MITRE ATT&CK 矩陣
MITRE ATT&CK Matrix for Containers
攻擊情境案例研究：弱點與濫用
Cases Study: Exploitable Vulnerabilities & Abuse the Legitimate Objects
稽核驅動資安
Audit Driven Security
理解CIS Kubernetes與Docker的評測基準
Outlines of the CIS Benchmarks with Kubernetes & Docker
CIS評測: 稽核缺失即錯誤設定
CIS Benchmarks: Audit Deficiencies as Misconfigurations
攻擊情境案例研究：錯誤設定
Cases Study: The Exploit to the Misconfigurations
防禦 Kubernetes
Defending Kubetnetes
使用MITRE D3FEND矩陣 將最佳實踐與控制措施加以分類
Mapping the Best Practices & Controls to MITRE D3FEND Matrix

Policies: Pod Security Standards

- 11 Level 1 Profile Checks, 2 Level 2 Profile Checks :

Pod Security Standards (PSS) are recommendations for securing deployed workloads to reduce the risks of container breakout. There are a number of ways if implementing PSS, including the built-in Pod Security Admission controller, or external policy control systems which integrate with Kubernetes via validating and mutating webhooks.

- Audit Deficiencies Implication:

Allows deployment of insecure pods (privileged, host access), enabling container escapes and node compromise.

攻擊者驅動資安
Adversary Driven Security
Kubernetes 與 Container Runtime 之威脅建模
Threat Modeling of Kubernetes & Container Runtime
容器化的 MITRE ATT&CK 矩陣
MITRE ATT&CK Matrix for Containers
攻擊情境案例研究：弱點與濫用
Cases Study: Exploitable Vulnerabilities & Abuse the Legitimate Objects
稽核驅動資安
Audit Driven Security
理解CIS Kubernetes與Docker的評測基準
Outlines of the CIS Benchmarks with Kubernetes & Docker
CIS評測: 稽核缺失即錯誤設定
CIS Benchmarks: Audit Deficiencies as Misconfigurations
攻擊情境案例研究：錯誤設定
Cases Study: The Exploit to the Misconfigurations
防禦 Kubernetes
Defending Kubetnetes
使用MITRE D3FEND矩陣將最佳實踐與控制措施加以分類
Mapping the Best Practices & Controls to MITRE D3FEND Matrix

Policies: Network Policies and CNI

- 1 Level 1 Profile Checks, 1 Level 2 Profile Checks:

Audits verify that a CNI plugin supporting Network Policies is installed, and then explicitly allowing necessary ingress/egress traffic. Crucially, it checks if policies are actually implemented, ideally starting with a default-deny policy for all namespaces isolate traffic in your cluster network.

- Audit Deficiencies Implication:

Lack of network segmentation allows unrestricted lateral movement within the cluster.

攻擊者驅動資安
Adversary Driven Security
Kubernetes 與 Container Runtime 之威脅建模
Threat Modeling of Kubernetes & Container Runtime
容器化的 MITRE ATT&CK 矩陣
MITRE ATT&CK Matrix for Containers
攻擊情境案例研究：弱點與濫用
Cases Study: Exploitable Vulnerabilities & Abuse the Legitimate Objects
稽核驅動資安
Audit Driven Security
理解CIS Kubernetes與Docker的評測基準
Outlines of the CIS Benchmarks with Kubernetes & Docker
CIS評測: 稽核缺失即錯誤設定
CIS Benchmarks: Audit Deficiencies as Misconfigurations
攻擊情境案例研究：錯誤設定
Cases Study: The Exploit to the Misconfigurations
防禦 Kubernetes
Defending Kubetnetes
使用MITRE D3FEND矩陣將最佳實踐與控制措施加以分類
Mapping the Best Practices & Controls to MITRE D3FEND Matrix

Policies: Secrets Management

- 2 Level 2 Profile Checks :

Kubernetes offers secrets via volumes or environment variables, but external secrets storage are preferred. For advanced needs, external secret managers with encryption and auditing are recommended.

- Audit Deficiencies Implication:

Sensitive data like API keys and passwords can be easily stolen by attackers with cluster access.

攻擊者驅動資安
Adversary Driven Security
Kubernetes 與 Container Runtime 之威脅建模
Threat Modeling of Kubernetes & Container Runtime
容器化的 MITRE ATT&CK 矩陣
MITRE ATT&CK Matrix for Containers
攻擊情境案例研究：弱點與濫用
Cases Study: Exploitable Vulnerabilities & Abuse the Legitimate Objects
稽核驅動資安
Audit Driven Security
理解CIS Kubernetes與Docker的評測基準
Outlines of the CIS Benchmarks with Kubernetes & Docker
CIS評測: 稽核缺失即錯誤設定
CIS Benchmarks: Audit Deficiencies as Misconfigurations
攻擊情境案例研究：錯誤設定
Cases Study: The Exploit to the Misconfigurations
防禦 Kubernetes
Defending Kubetnetes
使用MITRE D3FEND矩陣將最佳實踐與控制措施加以分類
Mapping the Best Practices & Controls to MITRE D3FEND Matrix

Policies: Extensible Admission Control

- 1 Level 2 Profile Checks:

Audits may check for the presence and configuration of validating or mutating admission webhooks that enforce custom security policies beyond built-in controls. Examples include webhooks for image provenance (ImagePolicyWebhook) or general policy engines like OPA Gatekeeper.

- Audit Deficiencies Implication:

Missed opportunities to enforce organization-specific security requirements at deployment time.

攻擊者驅動資安
Adversary Driven Security
Kubernetes 與 Container Runtime 之威脅建模
Threat Modeling of Kubernetes & Container Runtime
容器化的 MITRE ATT&CK 矩陣
MITRE ATT&CK Matrix for Containers
攻擊情境案例研究：弱點與濫用
Cases Study: Exploitable Vulnerabilities & Abuse the Legitimate Objects
稽核驅動資安
Audit Driven Security
理解CIS Kubernetes與Docker的評測基準
Outlines of the CIS Benchmarks with Kubernetes & Docker
CIS評測: 稽核缺失即錯誤設定
CIS Benchmarks: Audit Deficiencies as Misconfigurations
攻擊情境案例研究：錯誤設定
Cases Study: The Exploit to the Misconfigurations
防禦 Kubernetes
Defending Kubetnetes
使用MITRE D3FEND矩陣 將最佳實踐與控制措施加以分類
Mapping the Best Practices & Controls to MITRE D3FEND Matrix

Policies: General Policies

- 1 Level 1 Profile Checks, 3 Level 2 Profile Checks:

Audits aim to ensure better resource management and security within the Kubernetes cluster. This involves verifying the segregation of resources using namespaces, the enforcement of secure container configurations via SecComp profiles and Security Contexts, and the avoidance of the default namespace for enhanced control. Ultimately, these audits help in establishing administrative boundaries and applying security controls effectively at the namespace and pod/container levels.

- Audit Deficiencies Implication:

Workloads can consume excessive resources, potentially leading to DoS for other tenants or the node itself.

攻擊者驅動資安
Adversary Driven Security
Kubernetes 與 Container Runtime 之威脅建模
Threat Modeling of Kubernetes & Container Runtime
容器化的 MITRE ATT&CK 矩陣
MITRE ATT&CK Matrix for Containers
攻擊情境案例研究：弱點與濫用
Cases Study: Exploitable Vulnerabilities & Abuse the Legitimate Objects
稽核驅動資安
Audit Driven Security
理解CIS Kubernetes與Docker的評測基準
Outlines of the CIS Benchmarks with Kubernetes & Docker
CIS評測: 稽核缺失即錯誤設定
CIS Benchmarks: Audit Deficiencies as Misconfigurations
攻擊情境案例研究：錯誤設定
Cases Study: The Exploit to the Misconfigurations
防禦 Kubernetes
Defending Kubetnetes
使用MITRE D3FEND矩陣 將最佳實踐與控制措施加以分類
Mapping the Best Practices & Controls to MITRE D3FEND Matrix

CIS Docker Benchmark: Container Runtime Configuration (Req. 5.1~5.32)

- 28 Level 1 Profile Checks, 4 Level 2 Profile Checks:

The purpose of auditing the Container Runtime Configuration is to verify that containers are launched and operate with secure runtime parameters and configurations. This ensures that potential security vulnerabilities arising from insecure container execution settings are identified and mitigated, thereby protecting the host system and other containers. By auditing these configurations, organizations can confirm adherence to security best practices and internal security policies during the container runtime phase.

- Audit Deficiencies Implication:

Increasing the risk of vulnerability exploits and security breaches for the host system and other containers.

攻擊者驅動資安
Adversary Driven Security
Kubernetes 與 Container Runtime 之威脅建模
Threat Modeling of Kubernetes & Container Runtime
容器化的 MITRE ATT&CK 矩陣
MITRE ATT&CK Matrix for Containers
攻擊情境案例研究：弱點與濫用
Cases Study: Exploitable Vulnerabilities & Abuse the Legitimate Objects
稽核驅動資安
Audit Driven Security
理解CIS Kubernetes與Docker的評測基準
Outlines of the CIS Benchmarks with Kubernetes & Docker
CIS評測: 稽核缺失即錯誤設定
CIS Benchmarks: Audit Deficiencies as Misconfigurations
攻擊情境案例研究：錯誤設定
Cases Study: The Exploit to the Misconfigurations
防禦 Kubernetes
Defending Kubetnetes
使用MITRE D3FEND矩陣將最佳實踐與控制措施加以分類
Mapping the Best Practices & Controls to MITRE D3FEND Matrix

Cases Study: The Exploit to the Misconfigurations

CLOUD SECURITY Forum

Step	Attacker Action Description	Primary MITRE Tactic(s)	Primary MITRE Technique(s) (ID & Name)
1	Exploit exposed Kubelet API with anonymous auth	Initial Access	T1190 Exploit Public-Facing Application T1609 Container Administration Command
2	Execute command in pod via Kubelet API endpoint	Execution	T1609 Container Administration Command T1059 Command and Scripting Interpreter
3	Read pod's service account token from default mount path `cat /run/secrets/kubernetes.io/serviceaccount/token`	Credential Access	T1602 Data from Configuration Repository T1552 Unsecured Credentials
4	Discover service account's high privileges via API server query `curl -v -H "Authorization: Bearer <JWT_TOKEN>" https://<Kubernetes_API_IP>:<port>/api/v1/namespaces/default/secrets/`	Discovery Privilege Escalation for Permission Discovery	T1069 Permission Groups Discovery
5	Create privileged pod (privileged: true) with hostPath mount using stolen token	Privilege Escalation Lateral Movement	T1611 Escape to Host T1609 Container Administration Command
6	Execute commands in privileged pod, chroot to host filesystem	Privilege Escalation	T1611 Escape to Host
7	Access node-level credentials (/var/lib/kubelet/kubeconfig, cloud IMDS)	Credential Access Lateral Movement	T1552 Unsecured Credentials T1552.001 Credentials In Files, T1552.007 Cloud Instance Metadata API
8	Deploy persistence (DaemonSet), move laterally, Impact (mine)	Persistence Lateral Movement Impact	T1609 Container Administration Command T1496 Resource Hijacking T1530 Data from Cloud Storage Object Use of stolen node/cloud credentials for lateral movement (various Enterprise techniques)

Defending Kubernetes: Best Practices & Controls
防禦Kubernetes: 最佳實踐與控制措施

攻擊者驅動資安

Adversary Driven Security

Kubernetes 與 Container Runtime 之威脅建模

Threat Modeling of Kubernetes & Container Runtime

容器化的 MITRE ATT&CK 矩陣

MITRE ATT&CK Matrix for Containers

攻擊情境案例研究：弱點與濫用

Cases Study: Exploitable Vulnerabilities & Abuse the Legitimate Objects

稽核驅動資安

Audit Driven Security

理解CIS Kubernetes與Docker的評測基準

Outlines of the CIS Benchmarks with Kubernetes & Docker

CIS評測: 稽核缺失即錯誤設定

CIS Benchmarks: Audit Deficiencies as Misconfigurations

攻擊情境案例研究：錯誤設定

Cases Study: The Exploit to the Misconfigurations

防禦 Kubernetes

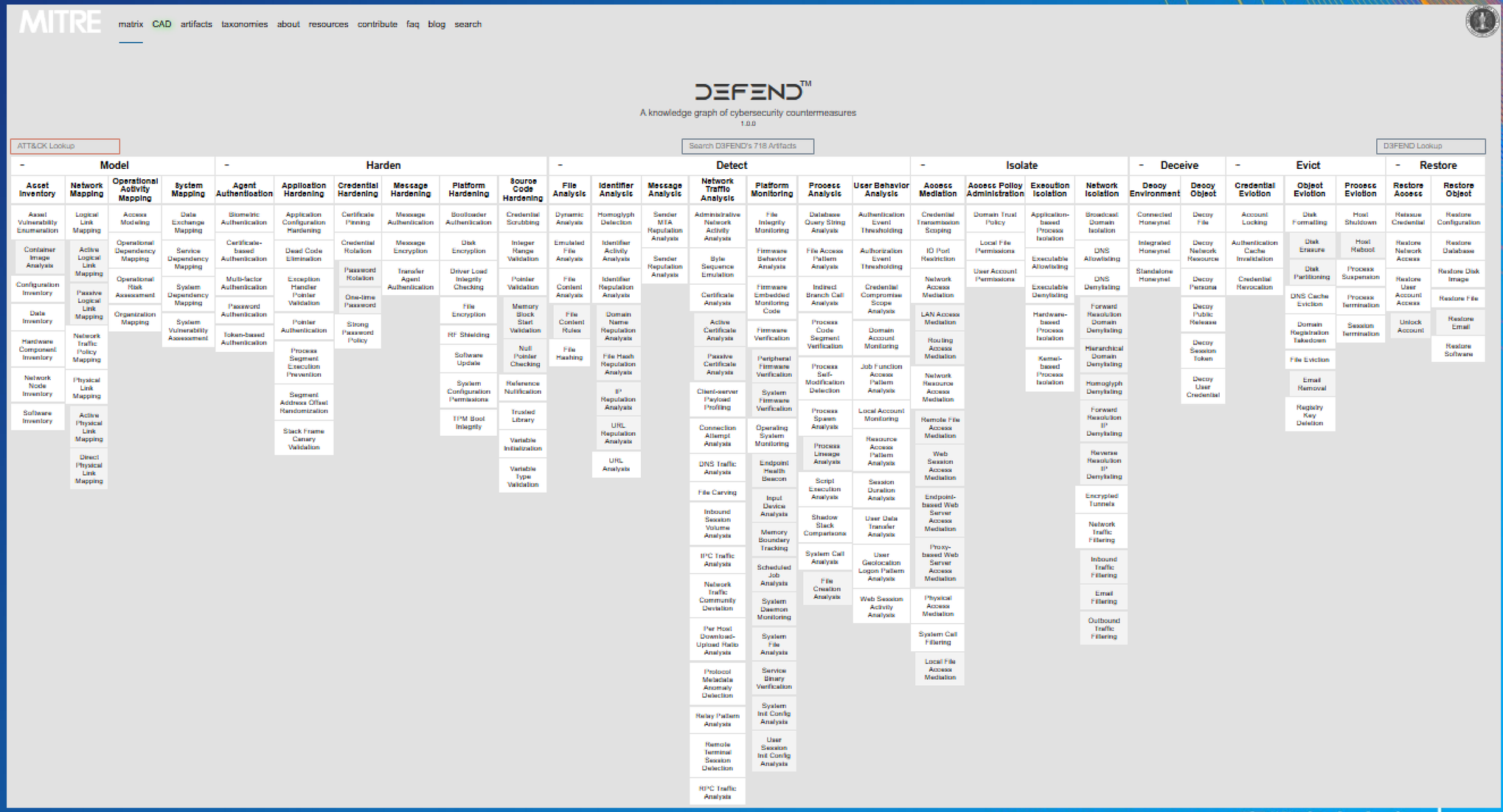
Defending Kubetnetes

使用MITRE D3FEND矩陣將最佳實踐與控制措施加以分類

Mapping the Best Practices & Controls to MITRE D3FEND Matrix

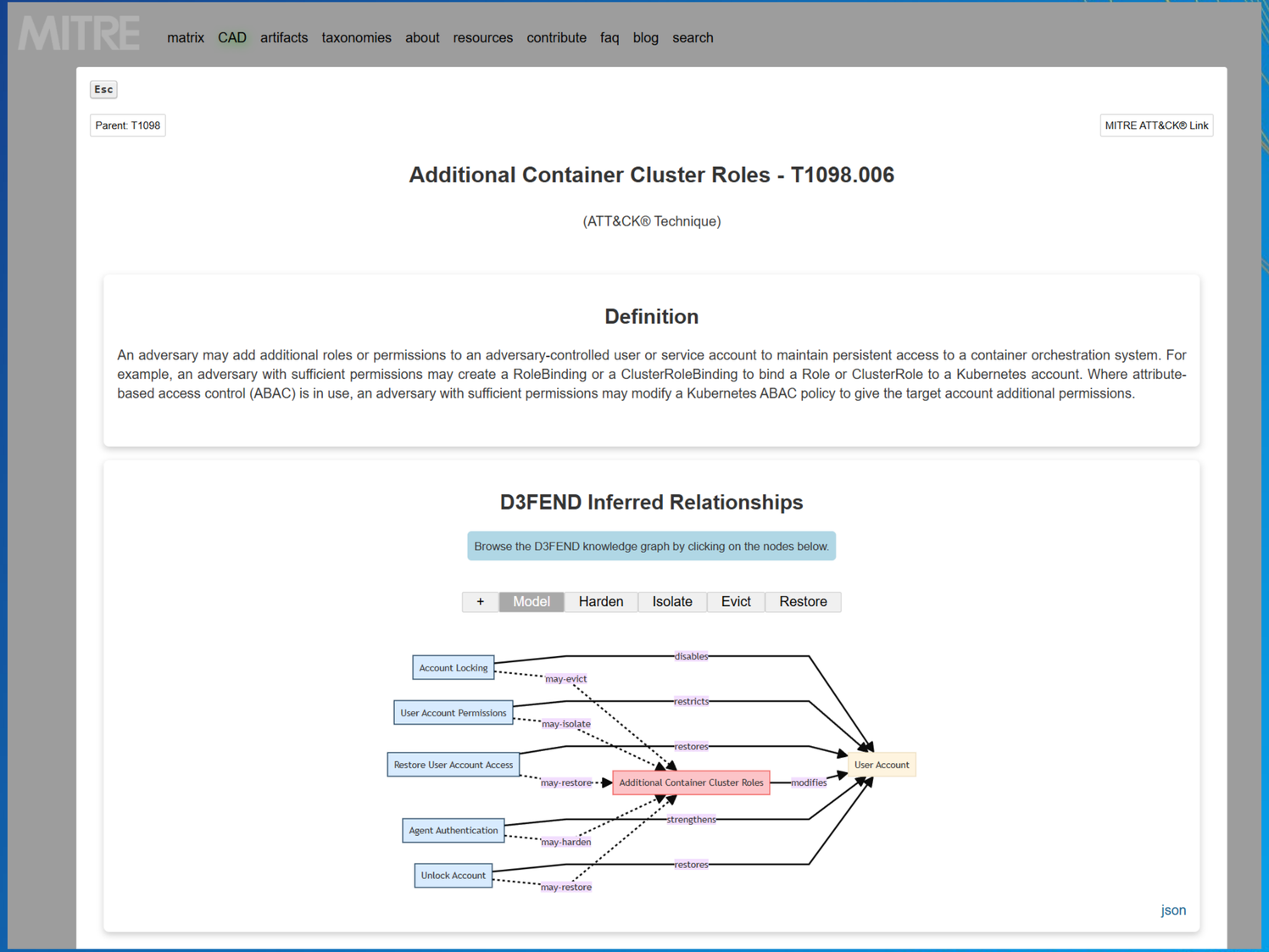
MITRE D3FEND Matrix

CLOUD SECURITY Forum



攻擊者驅動資安
Adversary Driven Security
Kubernetes 與 Container Runtime 之威脅建模
Threat Modeling of Kubernetes & Container Runtime
容器化的 MITRE ATT&CK 矩陣
MITRE ATT&CK Matrix for Containers
攻擊情境案例研究：弱點與濫用
Cases Study: Exploitable Vulnerabilities & Abuse the Legitimate Objects
稽核驅動資安
Audit Driven Security
理解CIS Kubernetes與Docker的評測基準
Outlines of the CIS Benchmarks with Kubernetes & Docker
CIS評測: 稽核缺失即錯誤設定
CIS Benchmarks: Audit Deficiencies as Misconfigurations
攻擊情境案例研究：錯誤設定
Cases Study: The Exploit to the Misconfigurations
防禦 Kubernetes
Defending Kubetnetes
使用MITRE D3FEND矩陣將最佳實踐與控制措施加以分類
Mapping the Best Practices & Controls to MITRE D3FEND Matrix

MITRE D3FEND Matrix



Mapping of D3FEND Concepts to Kubernetes Controls (Proactive)

D3FEND Tactic	D3FEND Technique	Relevant K8s Control/Practice
Model (建模)	Asset Inventory, Network Mapping, Operational Activity Mapping, System Mapping	**Image Scanning & Vulnerability Management**, **CIS Benchmark Auditing** (kube-bench), **IaC for Configuration Tracking**, **RBAC Auditing**, Network Policy Review, **Threat Modeling**, Resource Querying (kubectl get...), Service Mesh Visualization
Harden (強化)	Agent Authentication, Platform Hardening, Application Hardening, Credential Hardening, Message Hardening, Platform Hardening, Source Code Hardening	**Applying CIS Benchmarks**, **Pod Security Admission (PSA)**, **Security Profiles (Seccomp, SELinux, AppArmor)**, **Least Privilege RBAC**, Encrypting Secrets/etcd, **Image Scanning & Hardening**
Isolate (隔離)	Access Mediation, Access Policy Administration, Execution Isolation, Network Isolation	**Kubernetes Network Policies** (include isolation of etcd), **Namespaces** (logical isolation), **Pod Security Admission** (restricting host access), **Node Isolation** (taints/tolerations, separate node pools), **Container Runtimes** (basic isolation), Service Mesh (mTLS, L7 policies)

攻擊者驅動資安
Adversary Driven Security
Kubernetes 與 Container Runtime 之威脅建模
Threat Modeling of Kubernetes & Container Runtime
容器化的 MITRE ATT&CK 矩陣
MITRE ATT&CK Matrix for Containers
攻擊情境案例研究：弱點與濫用
Cases Study: Exploitable Vulnerabilities & Abuse the Legitimate Objects
稽核驅動資安
Audit Driven Security
理解CIS Kubernetes與Docker的評測基準
Outlines of the CIS Benchmarks with Kubernetes & Docker
CIS評測: 稽核缺失即錯誤設定
CIS Benchmarks: Audit Deficiencies as Misconfigurations
攻擊情境案例研究：錯誤設定
Cases Study: The Exploit to the Misconfigurations
防禦 Kubernetes
Defending Kubetnetes
使用MITRE D3FEND矩陣將最佳實踐與控制措施加以分類
Mapping the Best Practices & Controls to MITRE D3FEND Matrix

Mapping of D3FEND Concepts to Kubernetes Controls (Reactive)

D3FEND Tactic	D3FEND Technique	Relevant K8s Control/Practice
Detect (偵測)	Identifier Analysis, Network Traffic Analysis, File Analysis, Message Analysis, Platform Monitoring, Process Analysis, User Behavior Analysis	**Monitoring Kubernetes Audit Logs**, **Runtime Security Monitoring** (Falco, Sysdig, Tetragon, Business Cloud EDR Product), **Image Scanning**, **Network Policy Logging**, SIEM Integration
Evict (驅逐)	Process Eviction, Credential Eviction, Object Eviction	**Deleting malicious Pods/Deployments** (kubectl delete), Revoking Service Account Tokens/Credentials), **Cordoning/Draining Nodes** (kubectl cordon/drain), **Applying restrictive Network Policies**
Restore (恢復)	Restore Access, Restore Object	Redeploying from **GitOps/IaC**, Restoring from **Backups**, Rolling back deployments
Deceive (欺敵)	Decoy Environment, Decoy Object	Kubernetes Honeypots (mimicking exposed APIs/services)

Summary

Defending Kubernetes:
Best Practices & Controls

Audit Driven Security
(稽核驅動資安)

Adversary Driven Security
(攻擊者驅動資安)

Proactive Hardening and
Isolation (主動強化和隔離)

Reactive Detection and
Response (被動偵測和響應)

Thanks you!
感謝！

TEAM CYBERSECURITY