空降危機

雲端攻防二三事

Presented by Boik, 林殿智

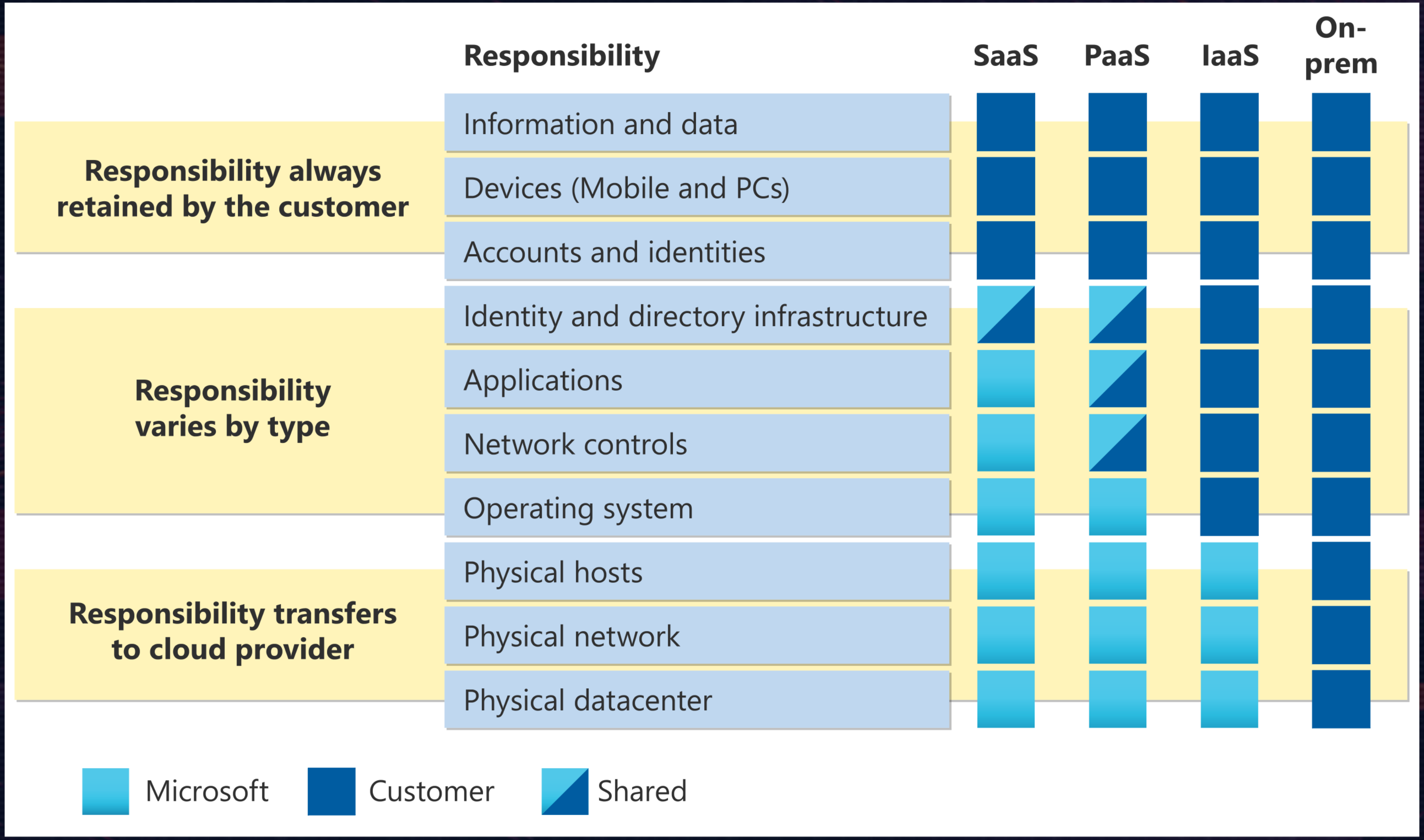
CYCRAFT

Outline

- Introduction
  - Cloud Security Alliance
  - Identity Perimeter
  - Network Perimeter
  - Hosted Applications/Services
- Case Study
  - AWS – Identity Perimeter
  - Azure – Network Perimeter
  - GCP – Hosted Applications/Services
- 藍隊工具整理

Introduction

Shared Responsibility Model



	Responsibility	SaaS	PaaS	IaaS	On-prem
Responsibility always retained by the customer	Information and data	■	■	■	■
	Devices (Mobile and PCs)	■	■	■	■
	Accounts and identities	■	■	■	■
Responsibility varies by type	Identity and directory infrastructure	◩	◩	■	■
	Applications	☐	◩	■	■
	Network controls	☐	◩	■	■
	Operating system	☐	☐	■	■
Responsibility transfers to cloud provider	Physical hosts	☐	☐	☐	■
	Physical network	☐	☐	☐	■
	Physical datacenter	☐	☐	☐	■

☐ Microsoft ■ Customer ◩ Shared

https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

“Through 2025, more than 99% of cloud breaches will have a root cause of preventable misconfigurations or mistakes by end users.”
- Gartner. (H/T Anton Chuvakin)

雲端威脅 – CSA 的觀點

- 1. Data Breaches
- 2. Misconfiguration and Inadequate Change Control
- 3. Lack of Cloud Security Architecture and Strategy
- 4. Insufficient Identity, Credential, Access and Key Management
- 5. Account Hijacking
- 6. Insider Threat
- 7. Insecure Interfaces and APIs
- 8. Weak Control Plane
- 9. Metastructure and Applistructure Failures
- 10. Limited Cloud Usage Visibility
- 11. Abuse and Nefarious Use of Cloud Services

https://cloudsecurityalliance.org/artifacts/top-threats-egregious-11-deep-dive/

雲端威脅 -三大面向

- >Identity Perimeter
- >Network Perimeter
- >Hosted Applications/Services

CYCRAFT

Identity Perimeter

- 身份與存取管理系統 (IAM) 過於複雜，難以管理
- 某些平台預設權限過高
- CSA Ref:
  - Data Breaches (No.1)
  - Insufficient Identity, Credential, Access and Key Management (No.4)
  - Account Hijacking (No.5)
  - Limited Cloud Usage Visibility (No.10)

雲端事件統計

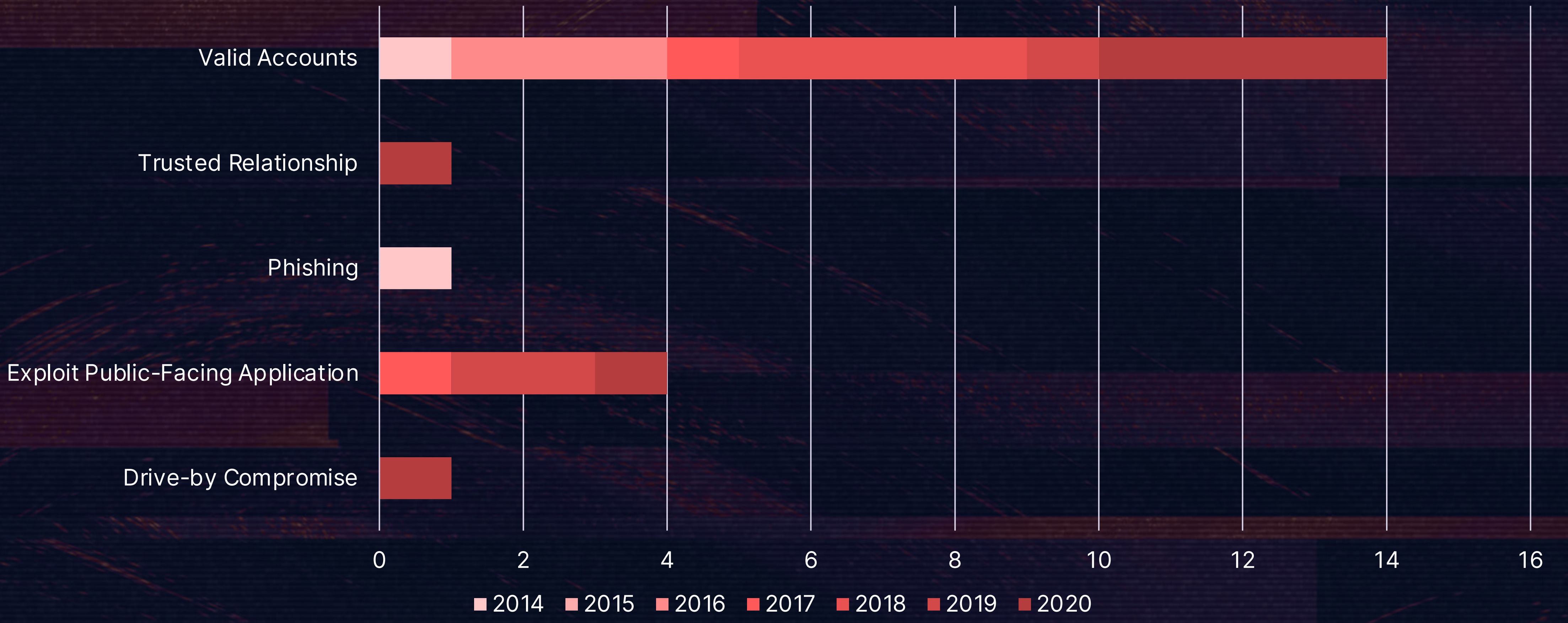
Learning from AWS Customer Security Incidents

Rami McCarthy

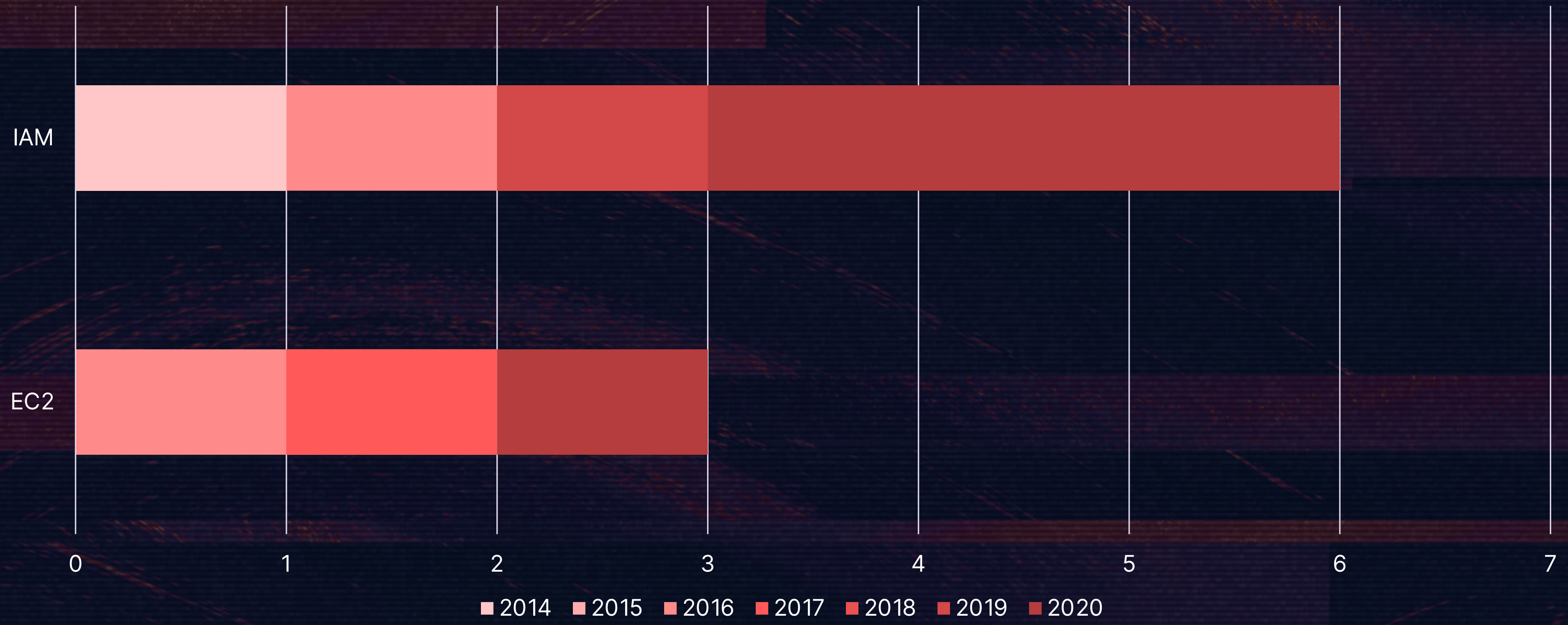
@ramimacisabird

https://speakerdeck.com/ramimac/learning-from-aws-customer-security-incidents

雲端事件 – Initial Access 統計



雲端事件 – Escalation/Persistence 統計



Network Perimeter

- 企業防禦邊界模糊化
- 雲地混合，信任關係
- CSA Ref:
  - Data Breaches (No.1)
  - Lack of Cloud Security Architecture and Strategy (No.3)
  - Insufficient Identity, Credential, Access and Key Management (No.4)
  - Weak Control Plane (No.8)

Hosted Applications/Services

- 過於複雜的應用程式設定
- 非原生雲端應用程式與雲端整合的問題
- CSA Ref:
  - Data Breaches (No.1)
  - Misconfiguration and Inadequate Change Control (No.2)
  - Insecure Interfaces and APIs (No.7)
  - Metastructure and Applistructure Failures (No.9)
  - Abuse and Nefarious Use of Cloud Services (No.11)

CYCRAFT

- >AWS: Identity Perimeter
- >Azure: Network Perimeter
- >GCP: Hosted Applications/Services

Case Study

AWS

Identity Perimeter

Identity and Access Management

Identity

Permission

Resource

Identity

User
Group
Service Account

Permission

Owner
Editor
Reader
…

Resource

VM
Bucket
…

	Identity	Permission	Resource
AWS	IAM User Federated Identity Resource (e.g. EC2, lambda) Identity from External Account IAM Group IAM Role	Policy (AWS / Customer Managed or Inline)	
GCP	Google Account Resource (e.g. CE, AE) Identity from External Account Google Group Google Workspace Domain Cloud Identity domain Service Account	Role (Basic / Custom) Role (Pre-define)	Resource
Azure	Azure User Application (e.g. x-account) Resource (e.g. VM, Function) Azure Group Service Principal Managed Identity	Role (Built-in / Custom)	Scope

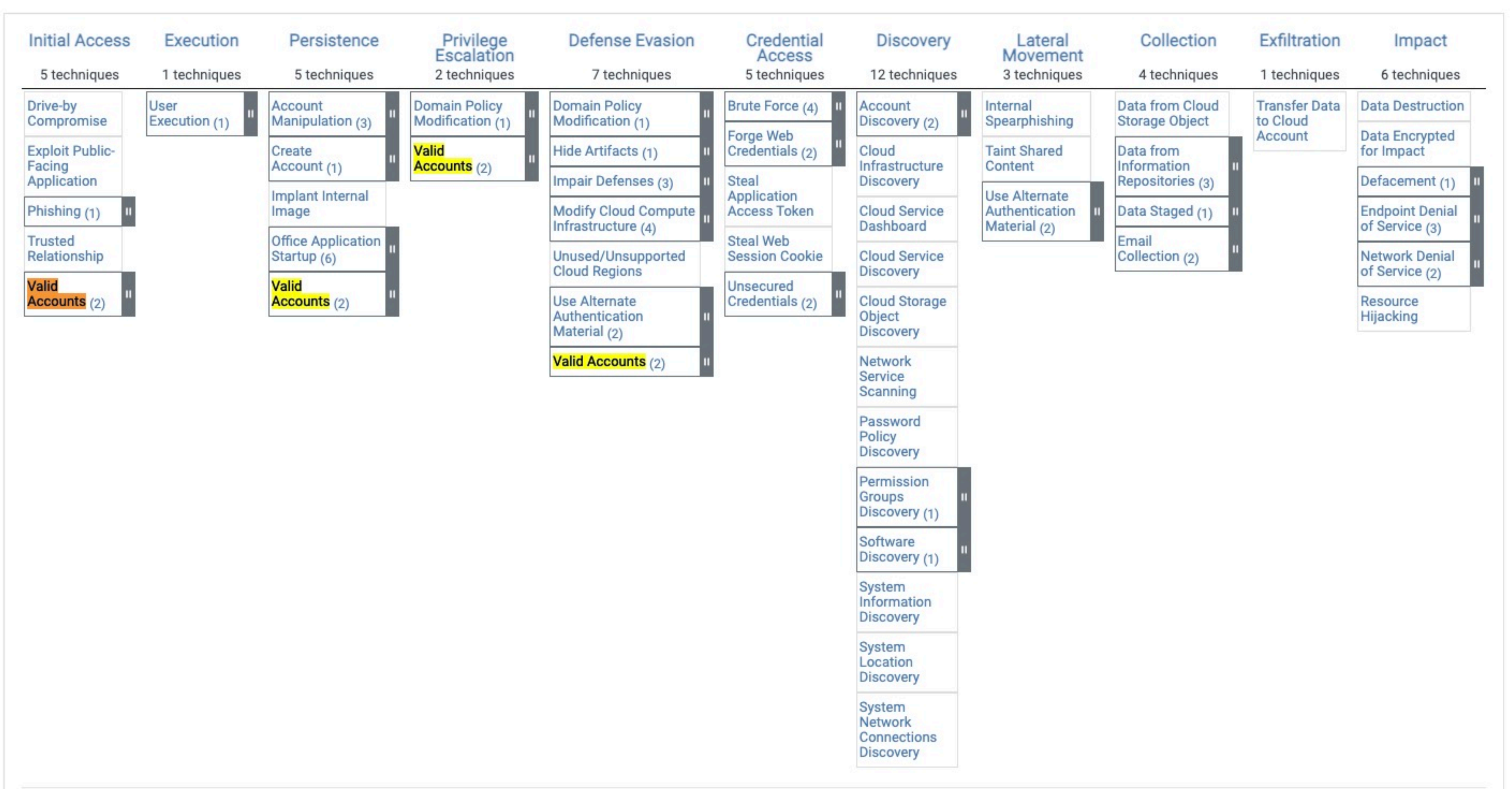
Legened: User Identity Service Identity User or Service Identity

Attack Mindset

- Credentials Harvest
- Lateral Movement
  - Add SSH key through control plane
  - Firewall rule enumeration
  - Bypassing boundaries
- Privilege Escalation
  - Modifying the metadata
  - Steal Credential from file, environment, code and control plane
  - Create IAM rule(Shadow Admin)

Credentials Harvest

- Internet-Facing Sensitive Data
- Config Files on Disk
- Control Plane Interface
- Codebase
- Environmental Variables



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Impact
5 techniques	1 techniques	5 techniques	2 techniques	7 techniques	5 techniques	12 techniques	3 techniques	4 techniques	1 techniques	6 techniques
Drive-by Compromise	User Execution (1)	Account Manipulation (3)	Domain Policy Modification (1)	Domain Policy Modification (1)	Brute Force (4)	Account Discovery (2)	Internal Spearphishing	Data from Cloud Storage Object	Transfer Data to Cloud Account	Data Destruction
Exploit Public-Facing Application		Create Account (1)	Valid Accounts (2)	Hide Artifacts (1)	Forge Web Credentials (2)	Cloud Infrastructure Discovery	Taint Shared Content	Data from Information Repositories (3)		Data Encrypted for Impact
Phishing (1)		Implant Internal Image		Impair Defenses (3)	Steal Application Access Token	Cloud Service Dashboard	Use Alternate Authentication Material (2)	Data Staged (1)		Defacement (1)
Trusted Relationship		Office Application Startup (6)		Modify Cloud Compute Infrastructure (4)	Steal Web Session Cookie	Cloud Service Discovery		Email Collection (2)		Endpoint Denial of Service (3)
Valid Accounts (2)		Valid Accounts (2)		Unused/Unsupported Cloud Regions	Unsecured Credentials (2)	Cloud Storage Object Discovery				Network Denial of Service (2)
				Use Alternate Authentication Material (2)		Network Service Scanning				Resource Hijacking
				Valid Accounts (2)		Password Policy Discovery				
						Permission Groups Discovery (1)				
						Software Discovery (1)				
						System Information Discovery				
						System Location Discovery				
						System Network Connections Discovery				

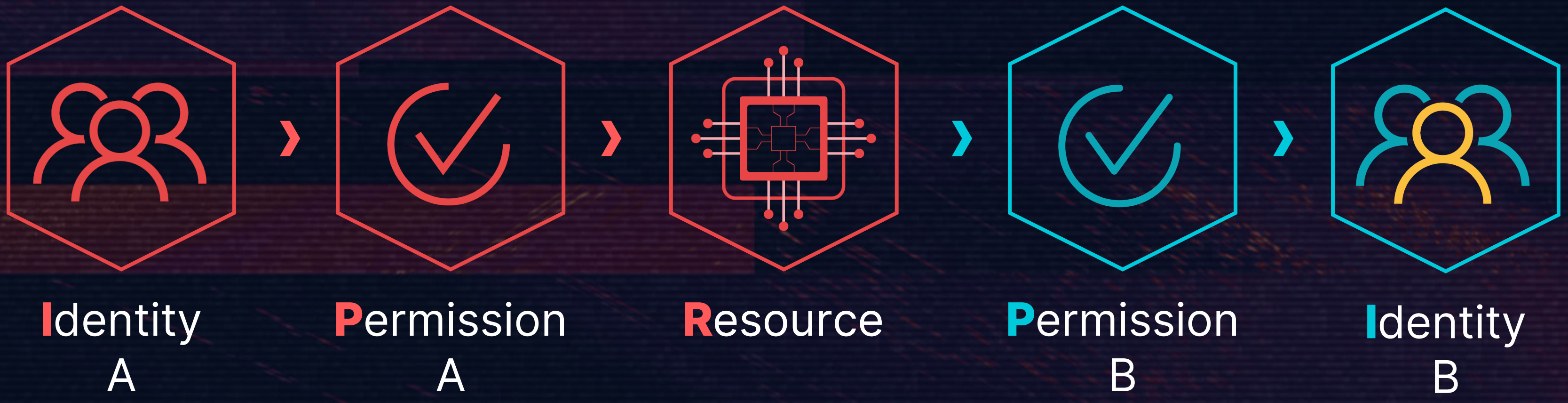
Cloud Matrix 對於 IAM 的利用過於粗略

Cloud Matrix 是大方向建議

The Lockheed killchain and MITRE ATT&CK models are two popular and well-developed frameworks, but they tend to be a bit high-level for guiding specific security control decisions. – DisruptOps

https://disruptops.com/stop-todays-top-10-cloud-attack-killchains/

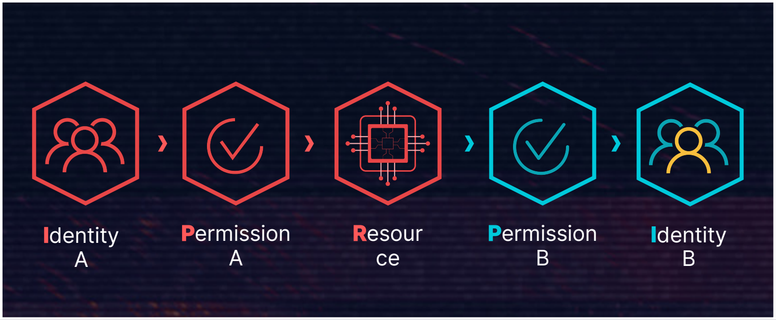
IAM Attack Pattern

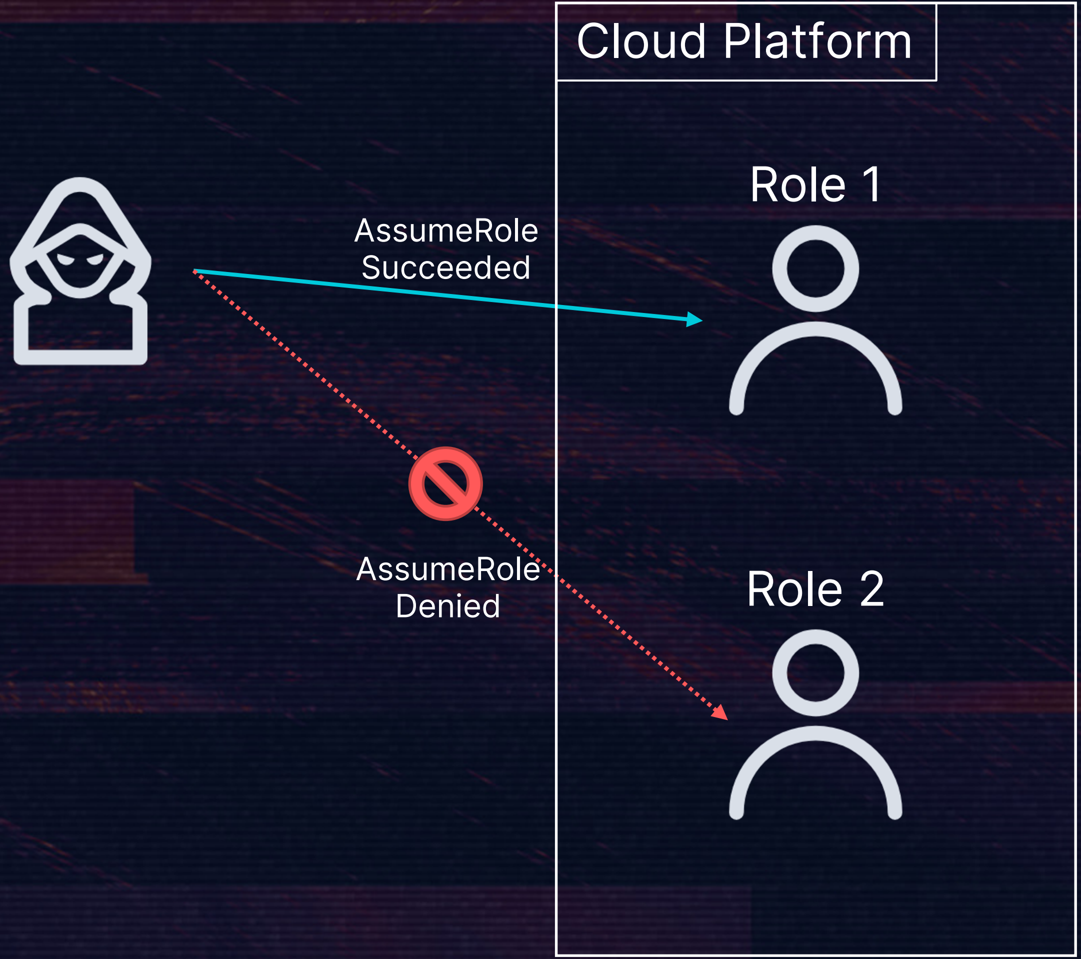


Identity A › Permission A › Resource › Permission B › Identity B

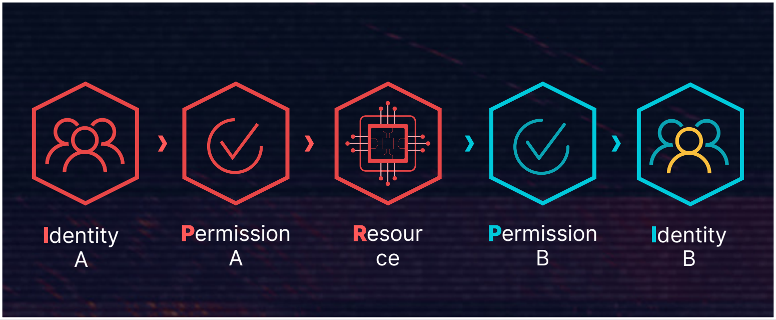
- S3 Resource Exposure / Sub-Domain Takeover
- 在 Instance 內翻 Code / Credential
- 借刀殺人（賦予權限給可控的 Resource）

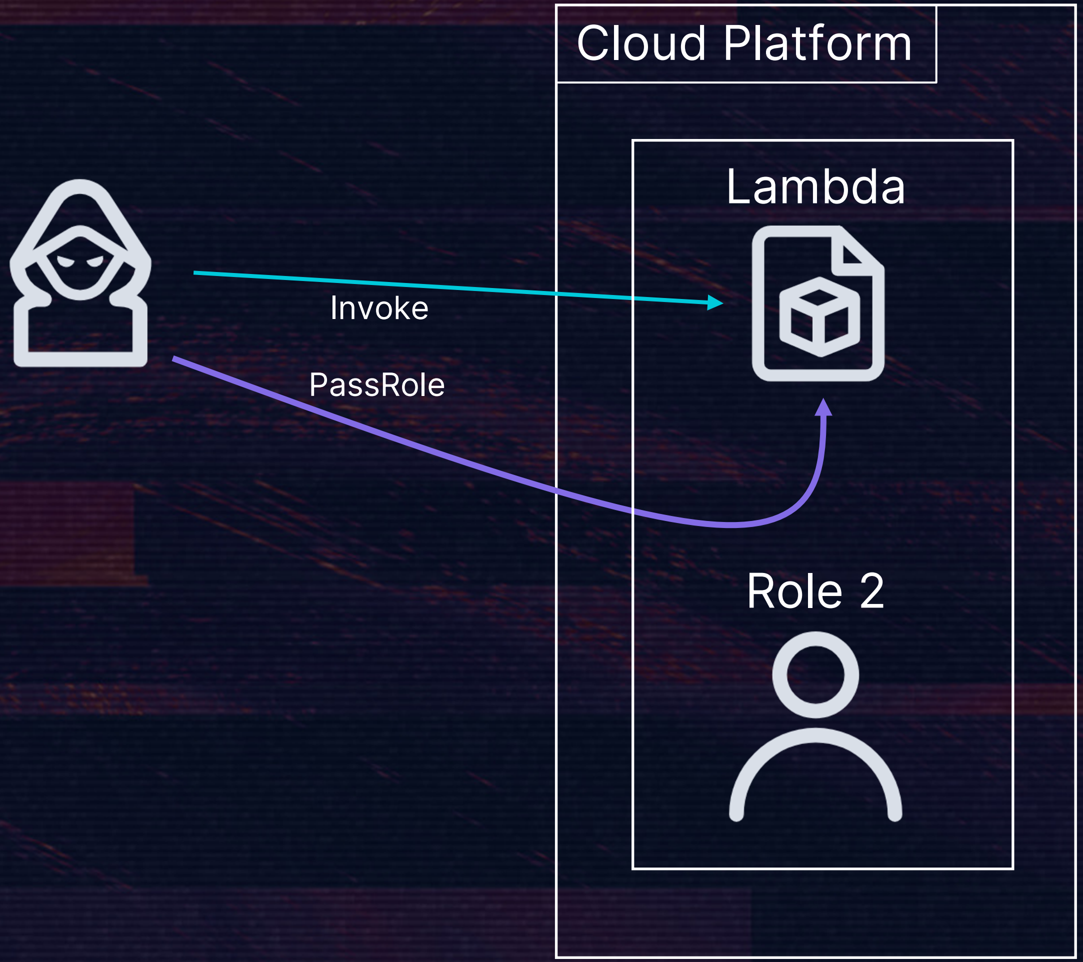
Credentials Harvest + LM

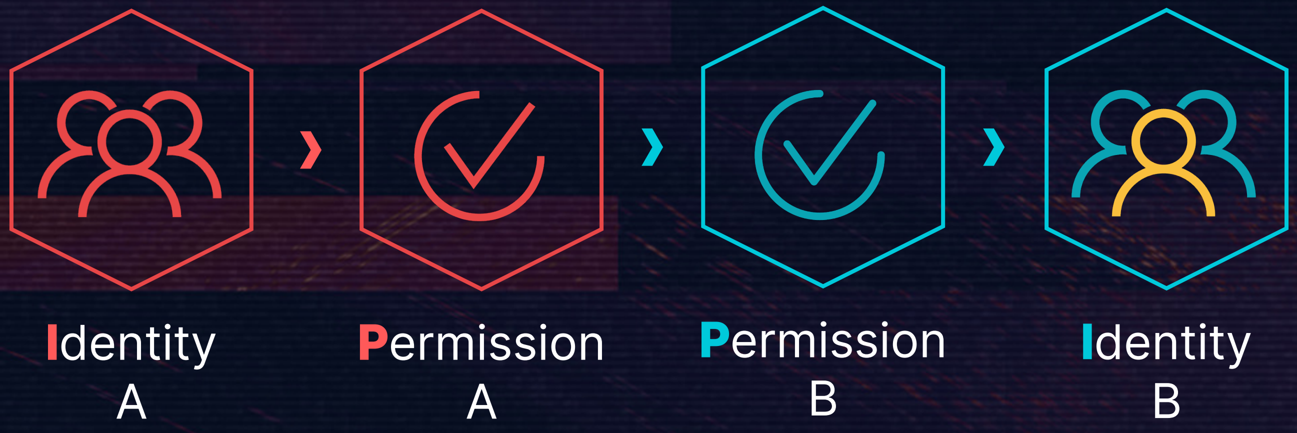




Privilege Escalation







Identity
A

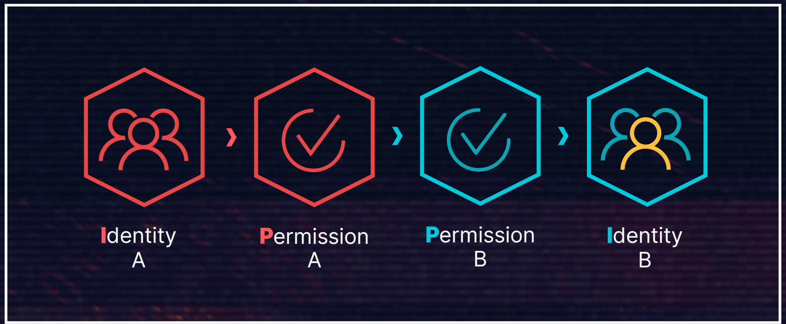
Permission
A

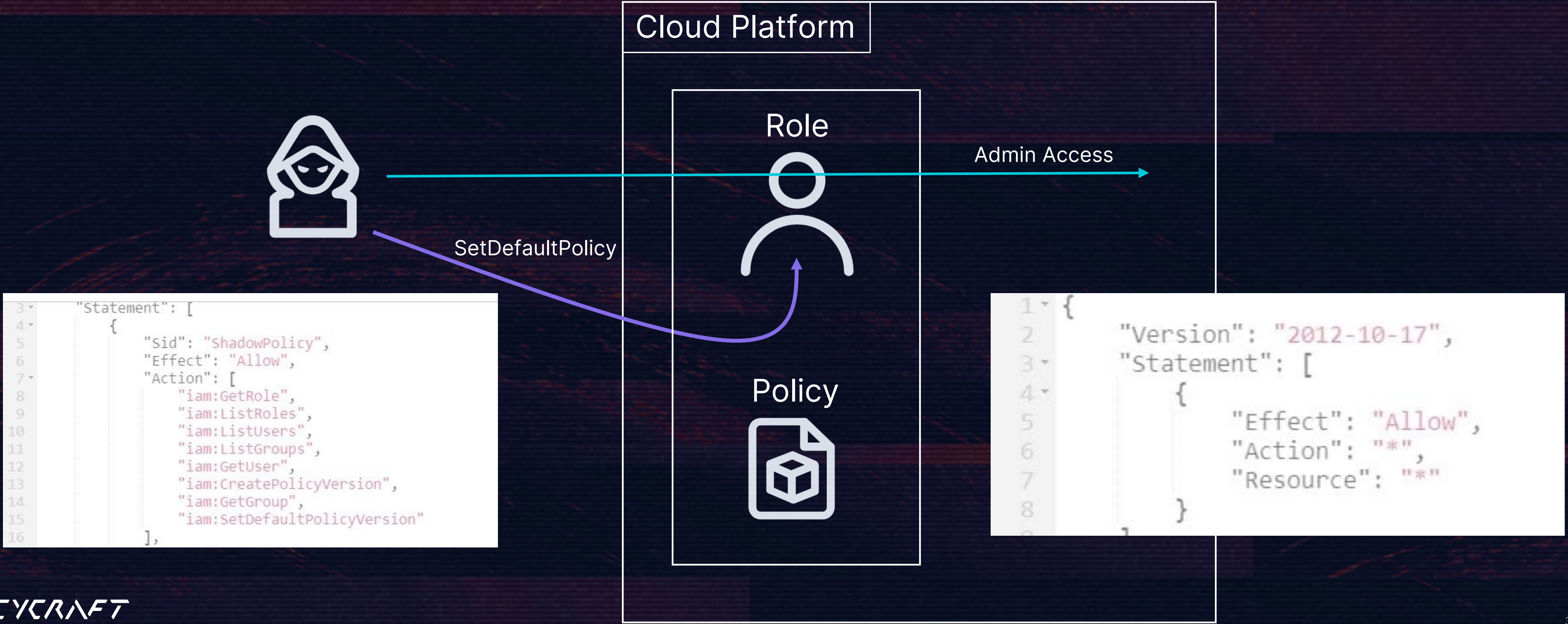
Permission
B

Identity
B

> 修改自身 Permission

Shadow Admin





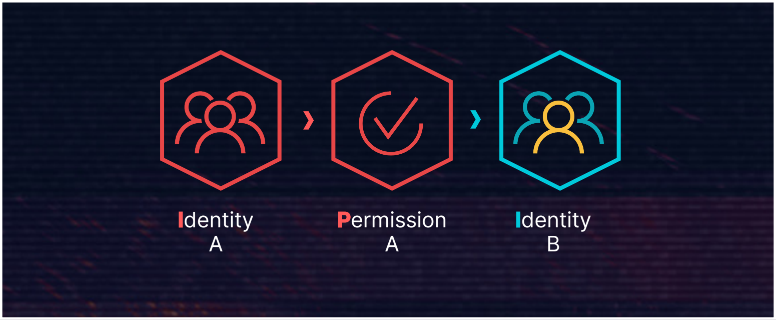
```
    "Statement": [
        {
            "Sid": "ShadowPolicy",
            "Effect": "Allow",
            "Action": [
                "iam:GetRole",
                "iam:ListRoles",
                "iam:ListUsers",
                "iam:ListGroups",
                "iam:GetUser",
                "iam:CreatePolicyVersion",
                "iam:GetGroup",
                "iam:SetDefaultPolicyVersion"
            ],
```

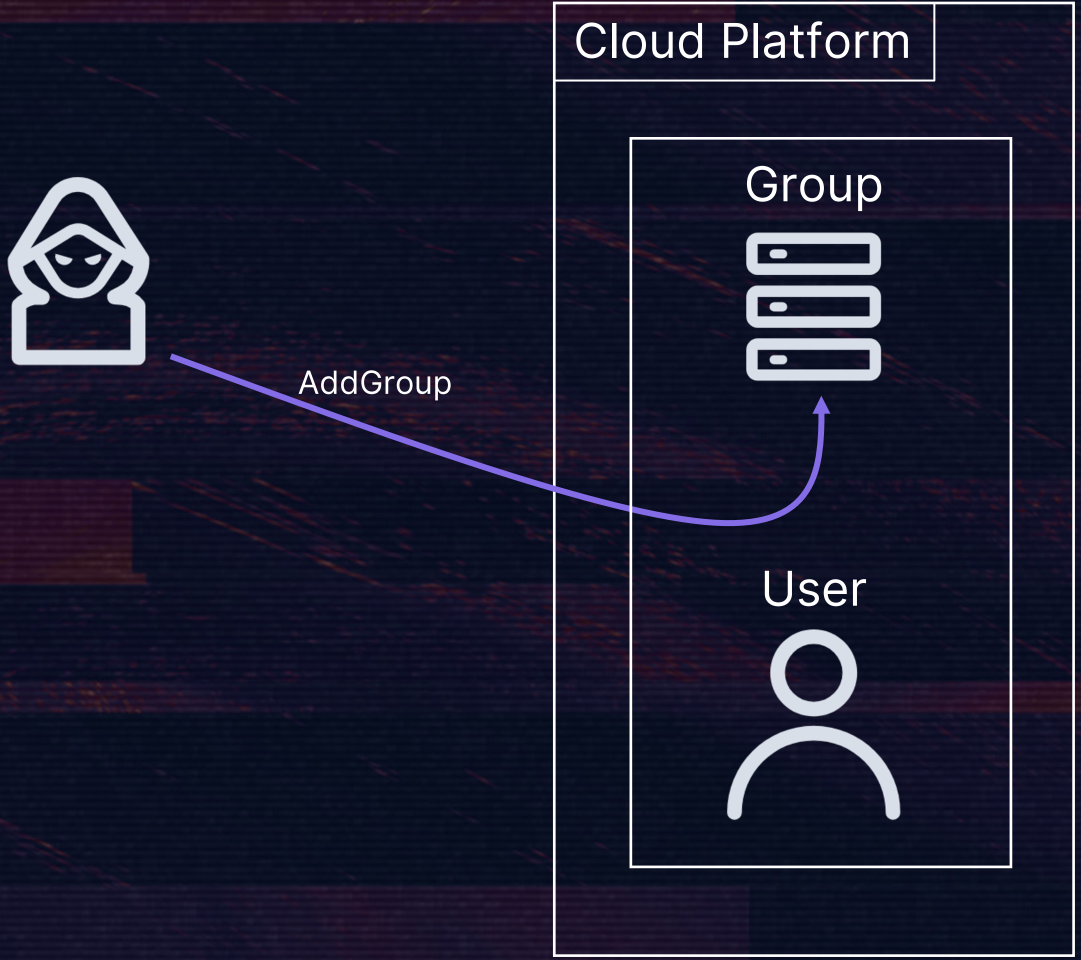
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*"
        }
    ]
```

Identity A › Permission A › Identity B

- 導出別的使用者的 Access key
- 改別的使用者的 login Profile
- 加到高權限 Group

Privilege Escalation



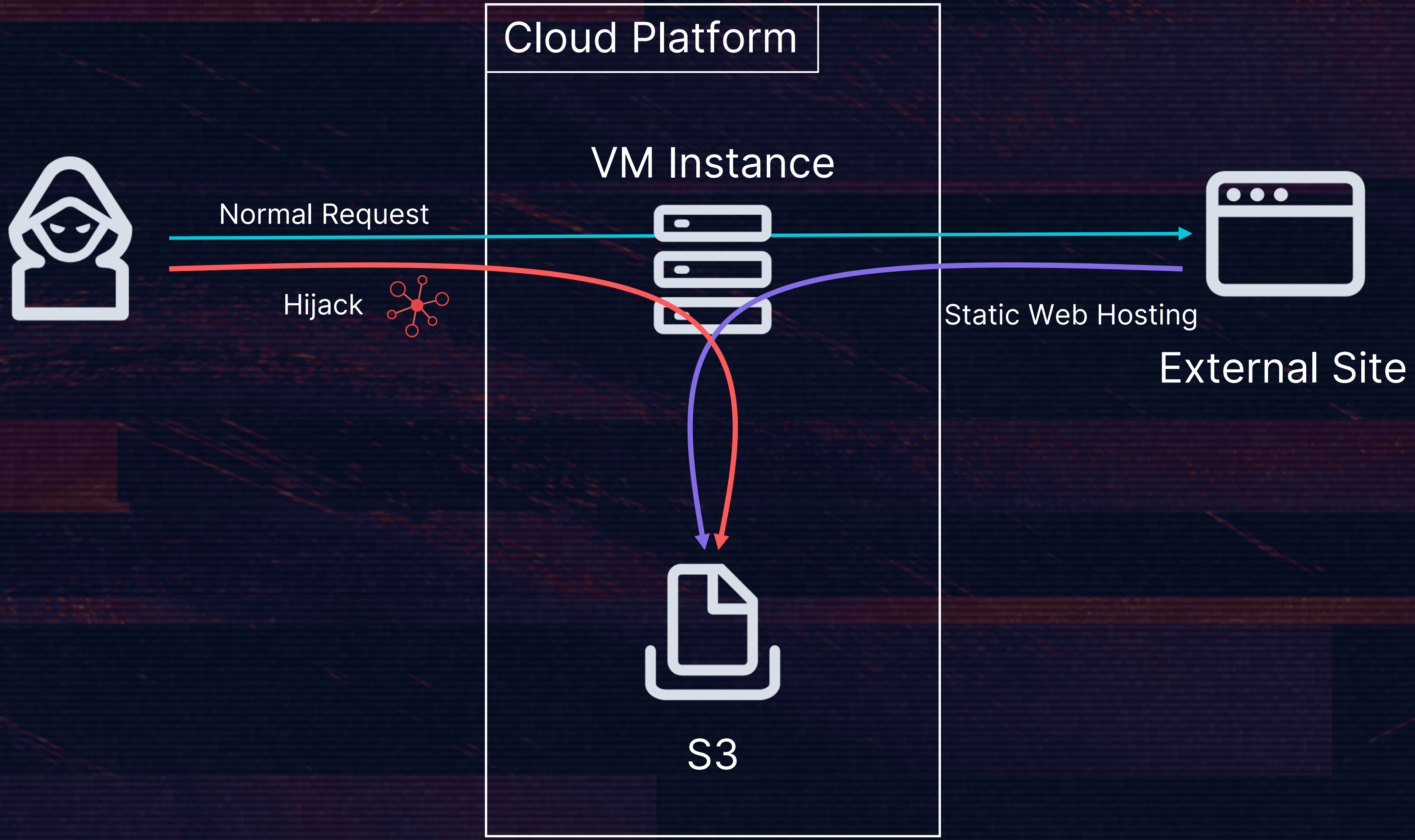


Resource A › Oracle › Identity B

> SSRF to Metadata Service

Sub-Domain Takeover + SSRF

Resource A
Oracle
Identity B

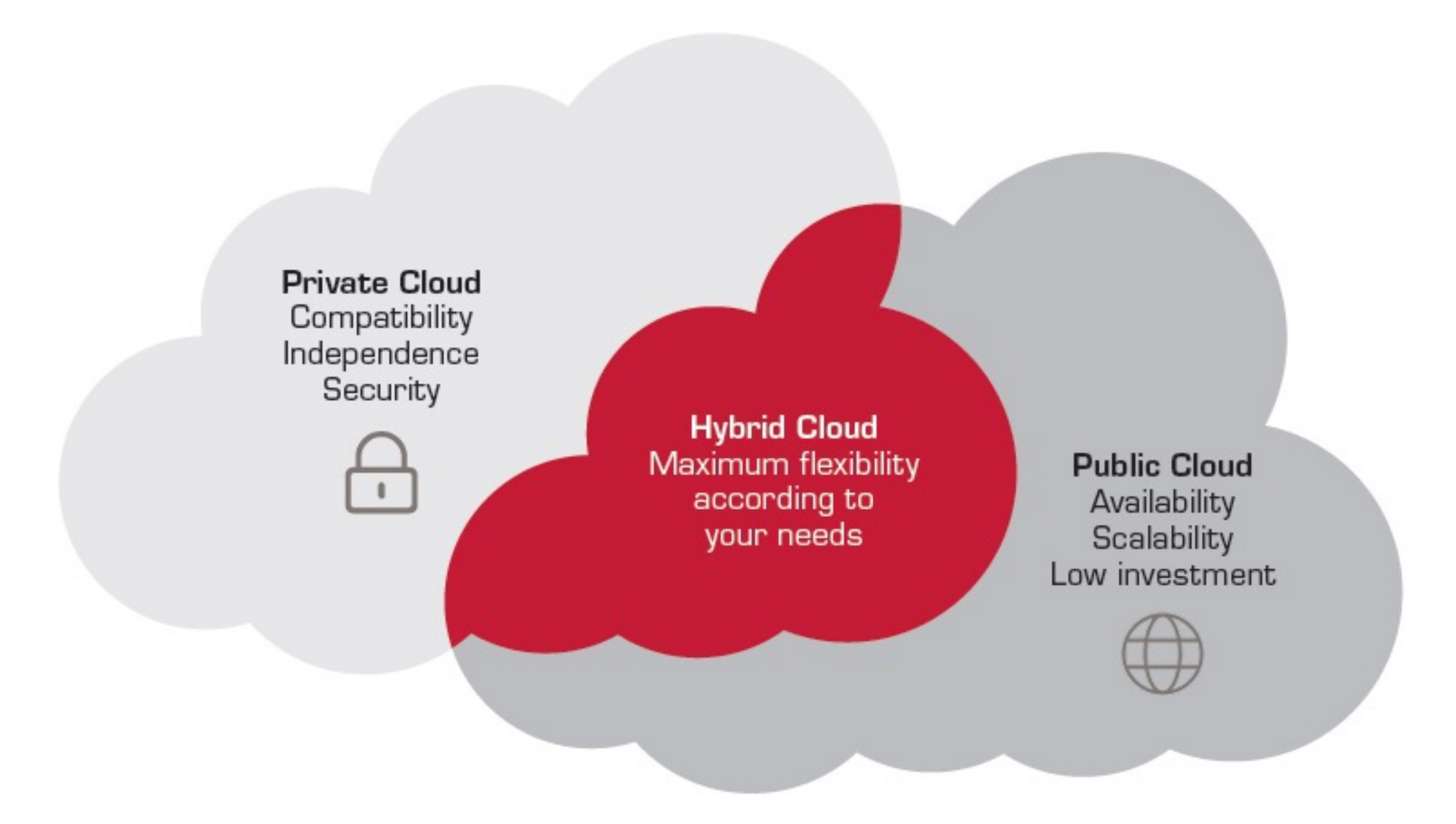


CyCraft

Azure

Network Perimeter

Private, Public and Hybrid Cloud



Private Cloud
Compatibility
Independence
Security

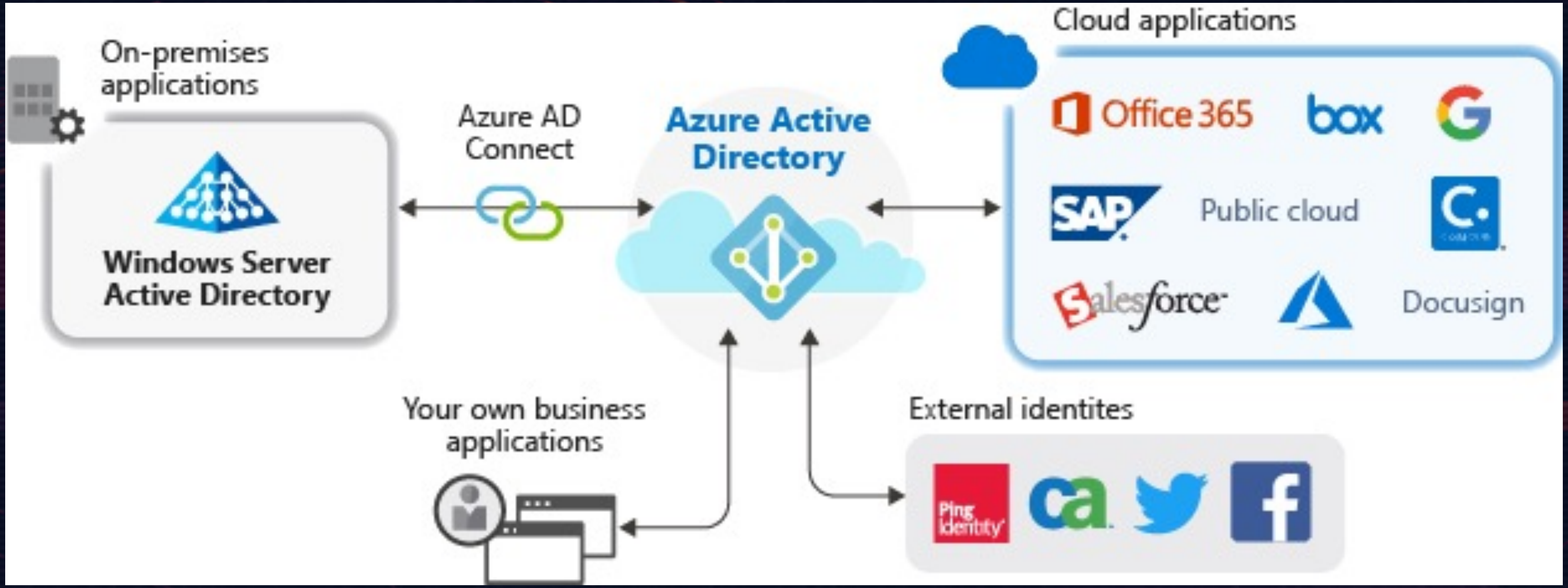
Hybrid Cloud
Maximum flexibility according to your needs

Public Cloud
Availability
Scalability
Low investment

https://itelligencegroup.com/cn/global-blog/what-is-a-hybrid-cloud/

Hybrid Cloud 的關鍵基礎設施

- Hybrid Identity for
  - Cross-realm Application Access
  - Simplified account access and management

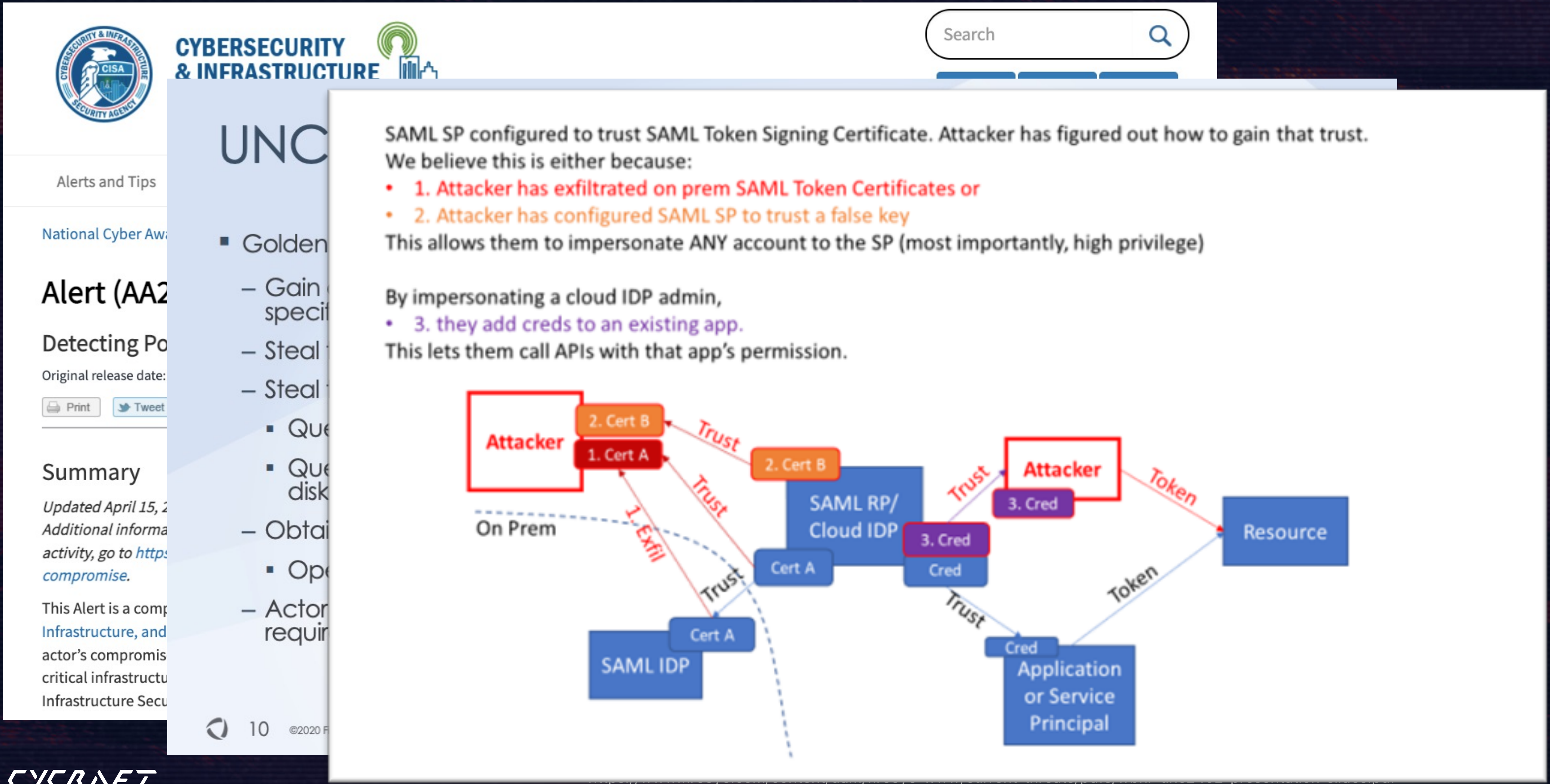


Active Directory vs. Azure AD

Active Directory	**Azure Active Directory**
LDAP	REST API’s
NTLM/Kerberos	OAuth/SAML/OpenID/etc
Structured directory (OU tree)	Flat structure
GPO’s	No GPO’s
Super fine-tuned access controls	Predefined roles
Domain/forest	Tenant
Trusts	Guests

https://troopers.de/downloads/troopers19/TROOPERS19_AD_Im_in_your_cloud.pdf

Real World Case - Solorigate



Search

CYBERSECURITY & INFRASTRUCTURE

Alerts and Tips

National Cyber Aw

Alert (AA2

Detecting Po

Original release date:

Print Tweet

Summary

Updated April 15, 2
Additional informa
activity, go to https
compromise.

This Alert is a comp
Infrastructure, and
actor's compromis
critical infrastructu
Infrastructure Secu

UNC

- Golden
  - Gain
    speci
  - Steal
  - Steal
    - Que
    - Que
      disk
  - Obtai
    - Op
  - Actor
    requir

10 ©2020 F

SAML SP configured to trust SAML Token Signing Certificate. Attacker has figured out how to gain that trust. We believe this is either because:

- 1. Attacker has exfiltrated on prem SAML Token Certificates or
- 2. Attacker has configured SAML SP to trust a false key

This allows them to impersonate ANY account to the SP (most importantly, high privilege)

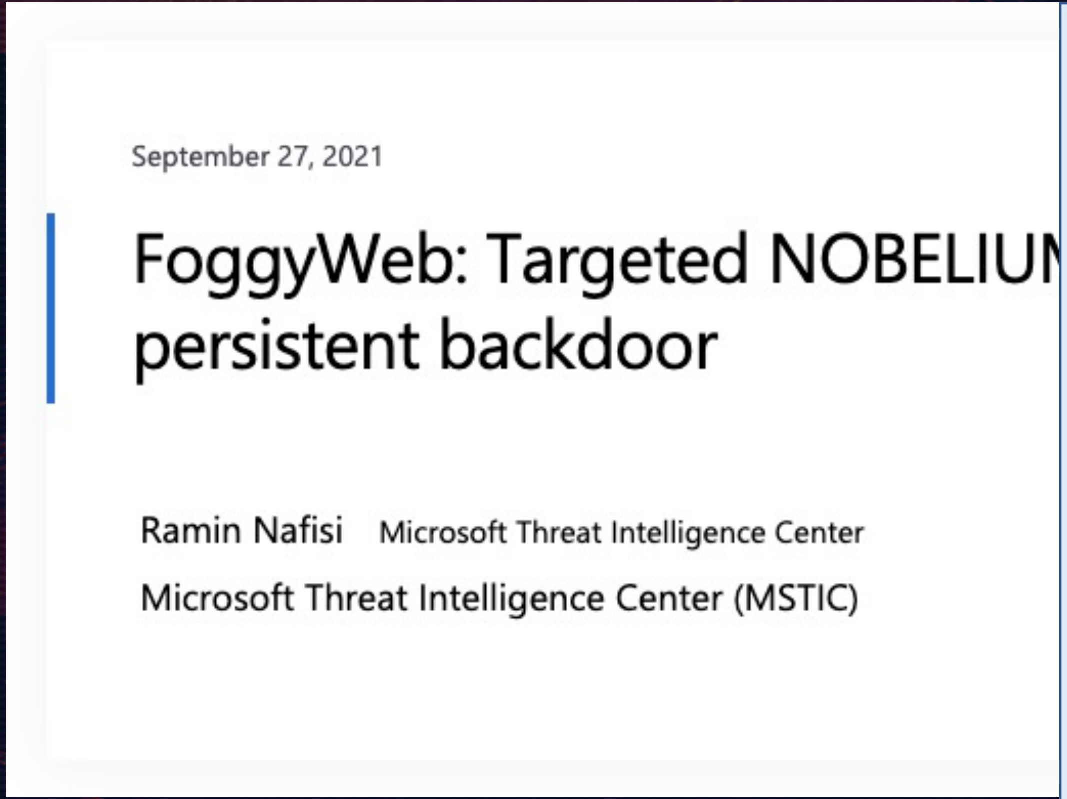
By impersonating a cloud IDP admin,

- 3. they add creds to an existing app.

This lets them call APIs with that app's permission.

https://techcommunity.microsoft.com/t5/azure-active-directory-identity/understanding-quot-solorigate-quot-s-identity-iocs-for-identity/ba-p/2007610

Real World Case - FoggyWeb

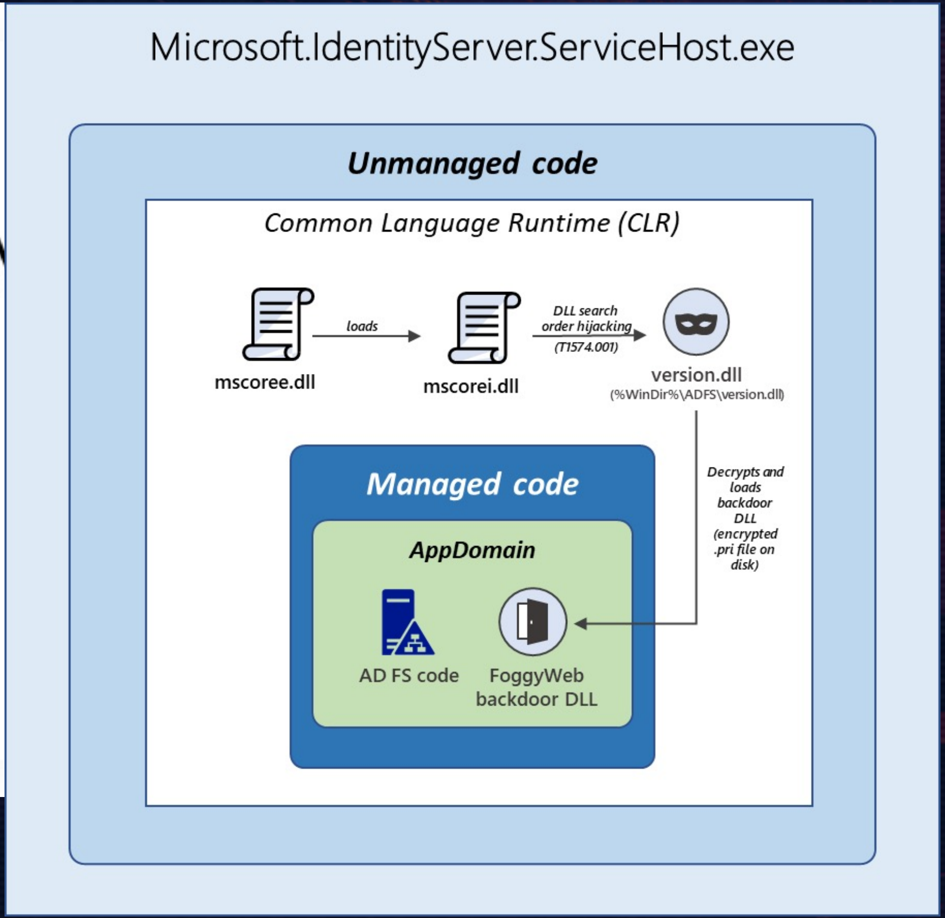


September 27, 2021

FoggyWeb: Targeted NOBELIU
persistent backdoor

Ramin Nafisi Microsoft Threat Intelligence Center

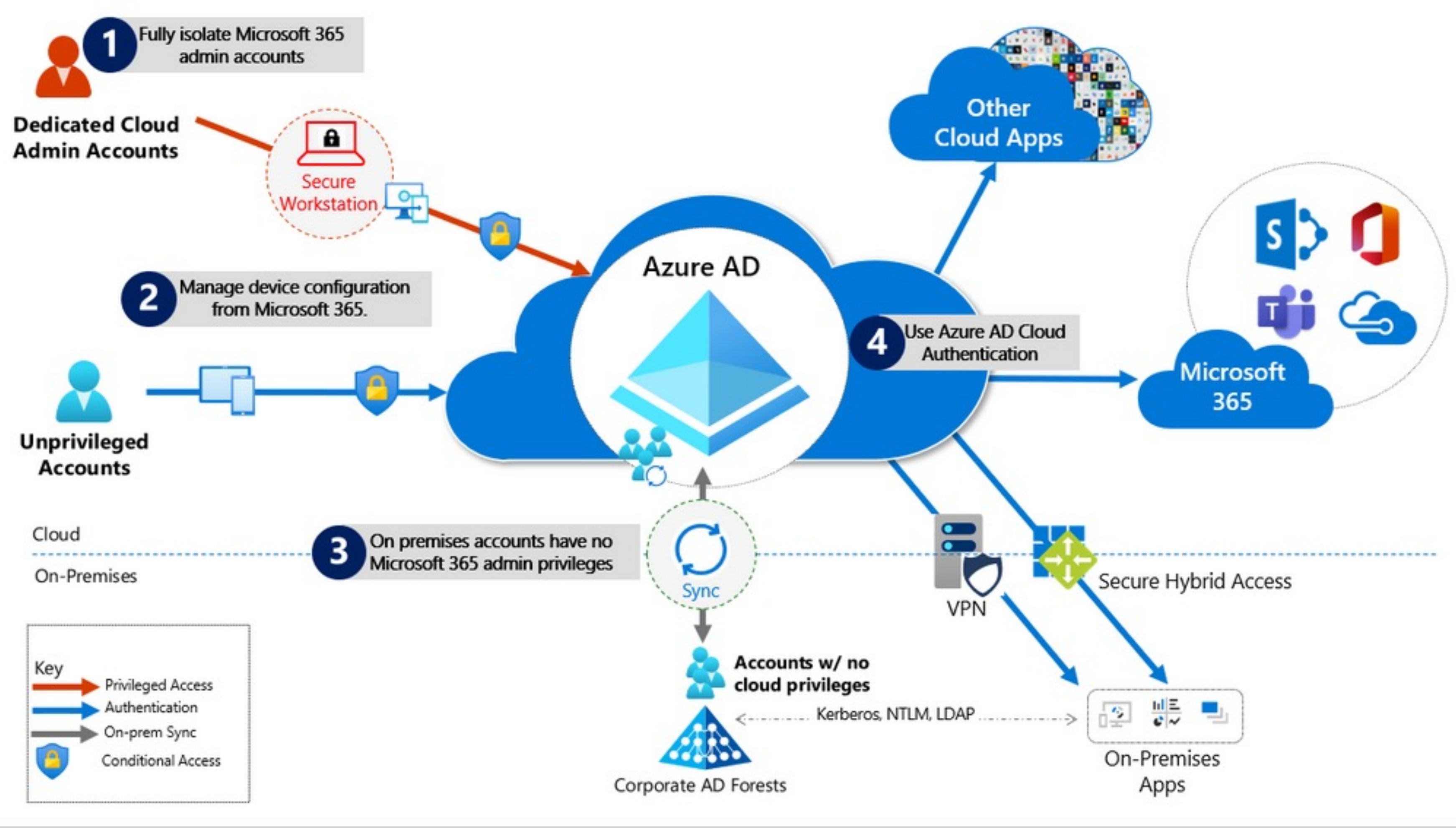
Microsoft Threat Intelligence Center (MSTIC)



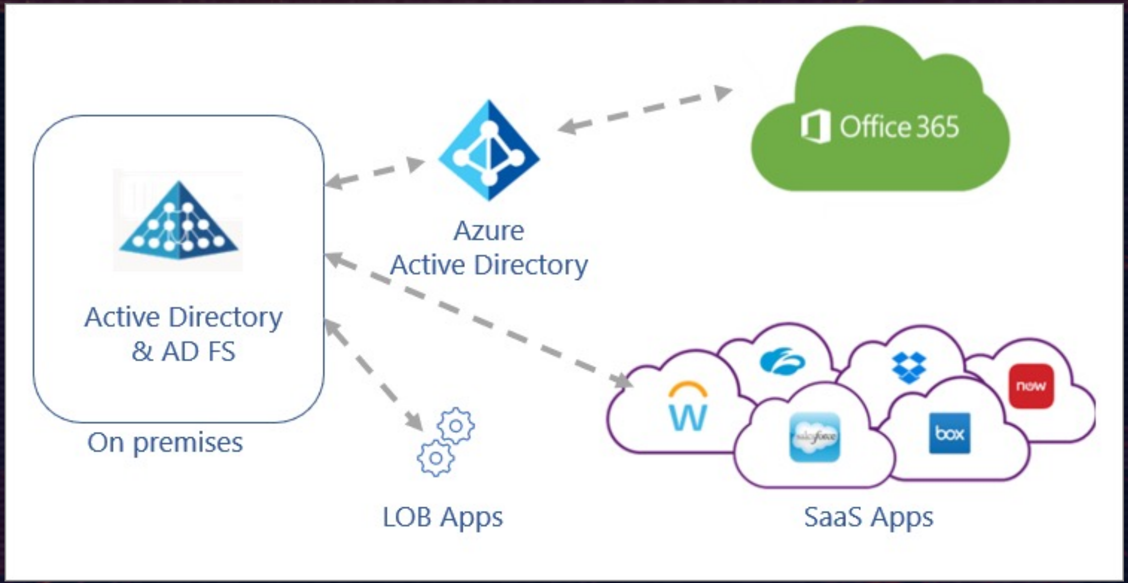
Microsoft.IdentityServer.ServiceHost.exe
Unmanaged code
Common Language Runtime (CLR)
mscoree.dll
loads
mscorei.dll
DLL search order hijacking (T1574.001)
version.dll
(%WinDir%\ADFS\version.dll)
Decrypts and loads backdoor DLL (encrypted .pri file on disk)
Managed code
AppDomain
AD FS code
FoggyWeb backdoor DLL

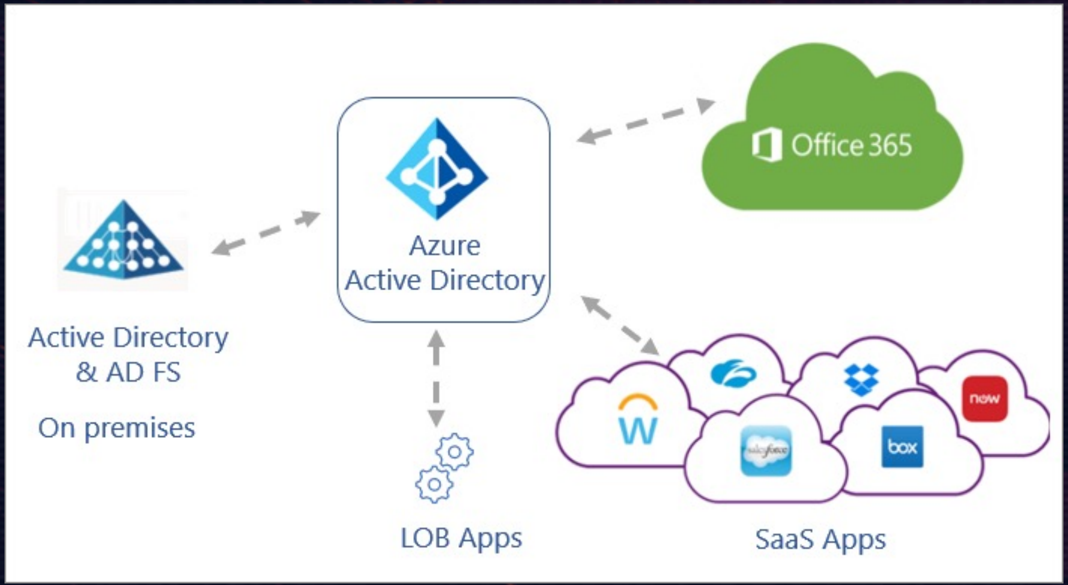
https://www.microsoft.com/security/blog/2021/09/27/foggyweb-targeted-nobelium-malware-leads-to-persistent-backdoor/

Best Practice


1 Fully isolate Microsoft 365 admin accounts
Dedicated Cloud Admin Accounts
Secure Workstation
2 Manage device configuration from Microsoft 365.
Unprivileged Accounts
Azure AD
Other Cloud Apps
4 Use Azure AD Cloud Authentication
Microsoft 365
Cloud
On-Premises
3 On premises accounts have no Microsoft 365 admin privileges
Sync
VPN
Secure Hybrid Access
Accounts w/ no cloud privileges
Kerberos, NTLM, LDAP
Corporate AD Forests
On-Premises Apps
Key
Privileged Access
Authentication
On-prem Sync
Conditional Access

https://techcommunity.microsoft.com/t5/azure-active-directory-identity/protecting-microsoft-365-from-on-premises-attacks/ba-p/1751754


Office 365
Azure
Active Directory
Active Directory
& AD FS
On premises
LOB Apps
SaaS Apps
new
box

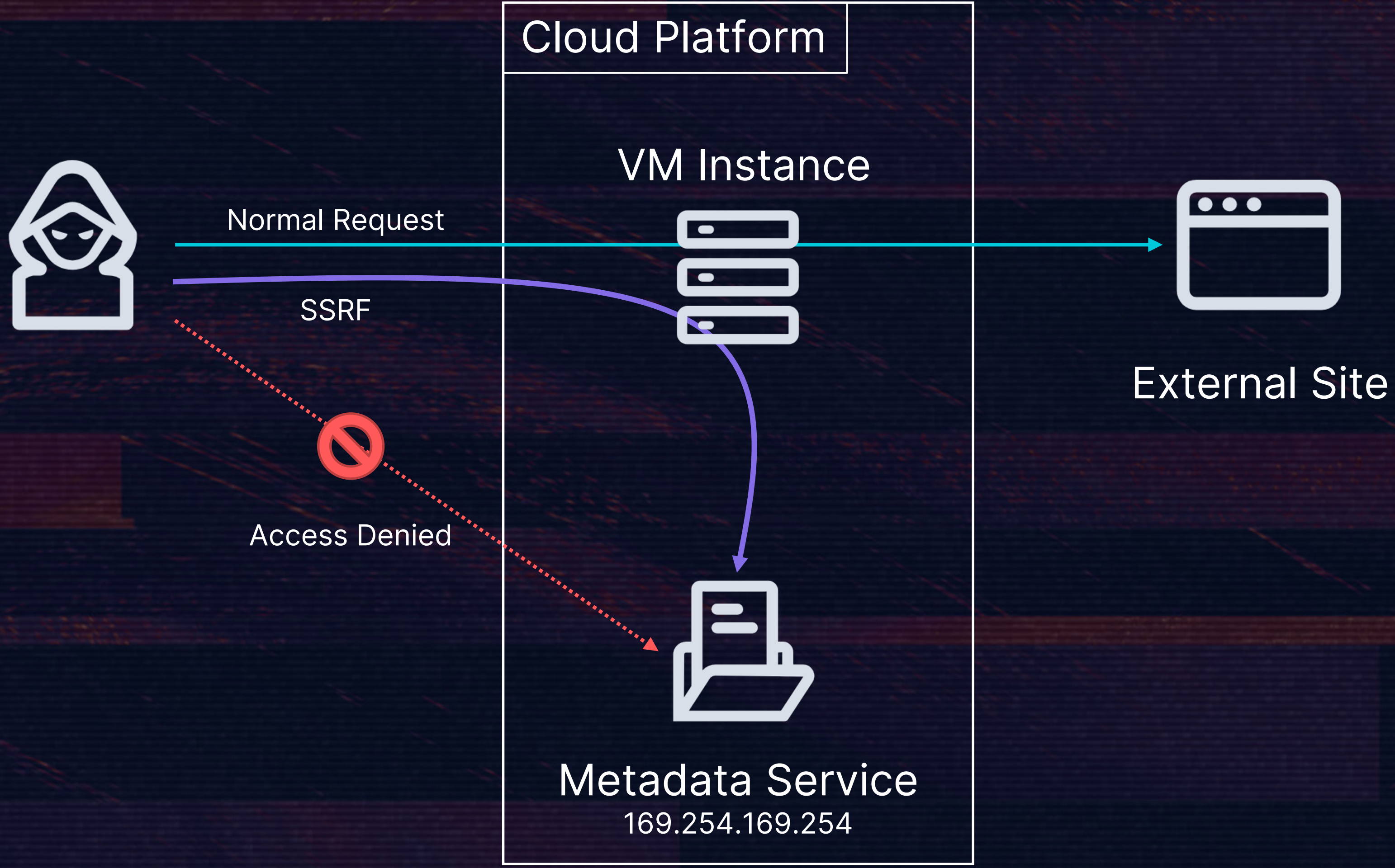

Office 365
Azure
Active Directory
Active Directory
& AD FS
On premises
LOB Apps
SaaS Apps
new
box

GCP

Hosted Applications/Services

Server Side Request Forgery

Resource
A
Oracle
Identity
B

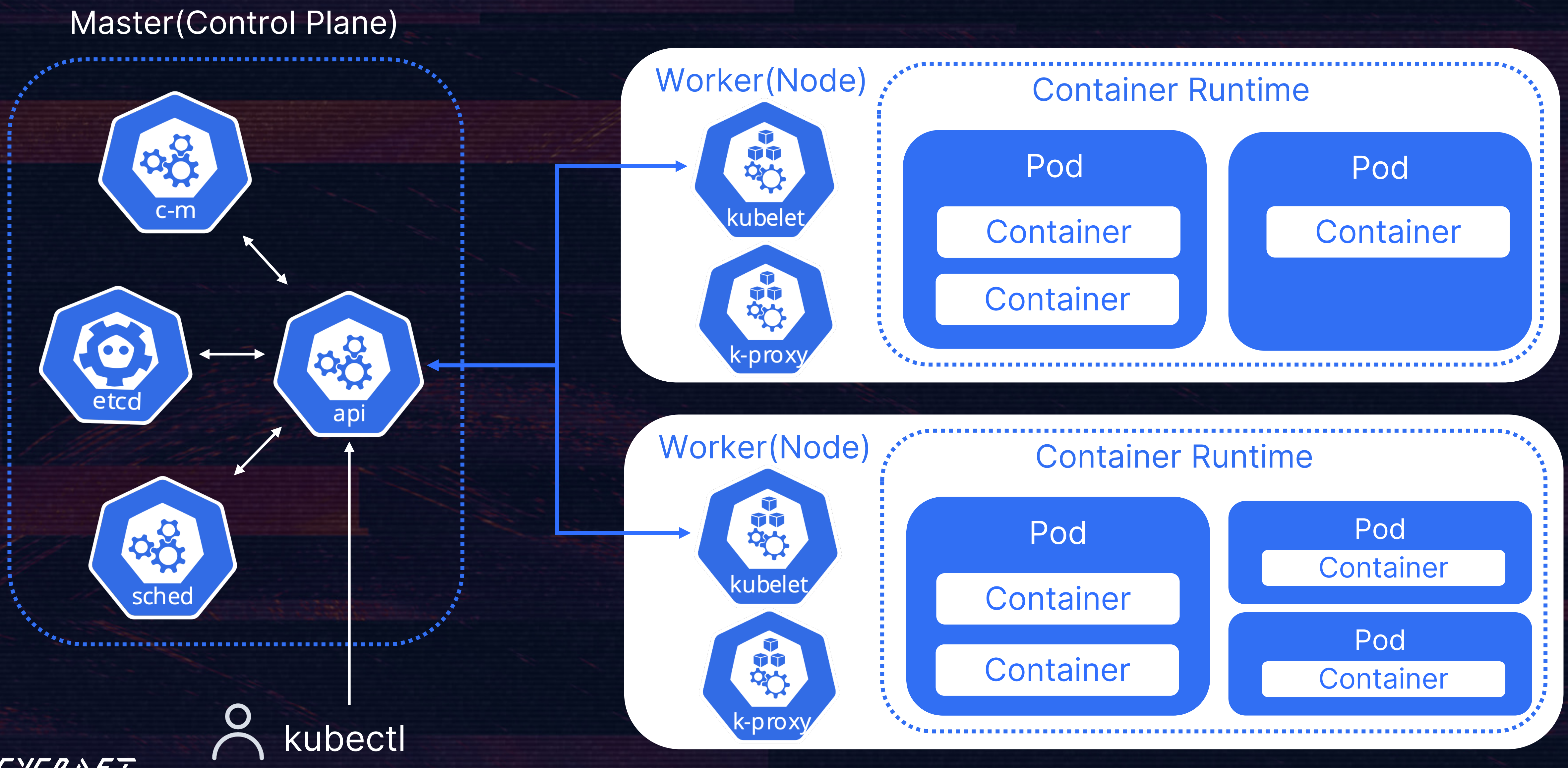


Root Cause

- Oracle（Instance Metadata Service） 缺乏身份驗證（Authentication）
- 無法區別請求由誰發出

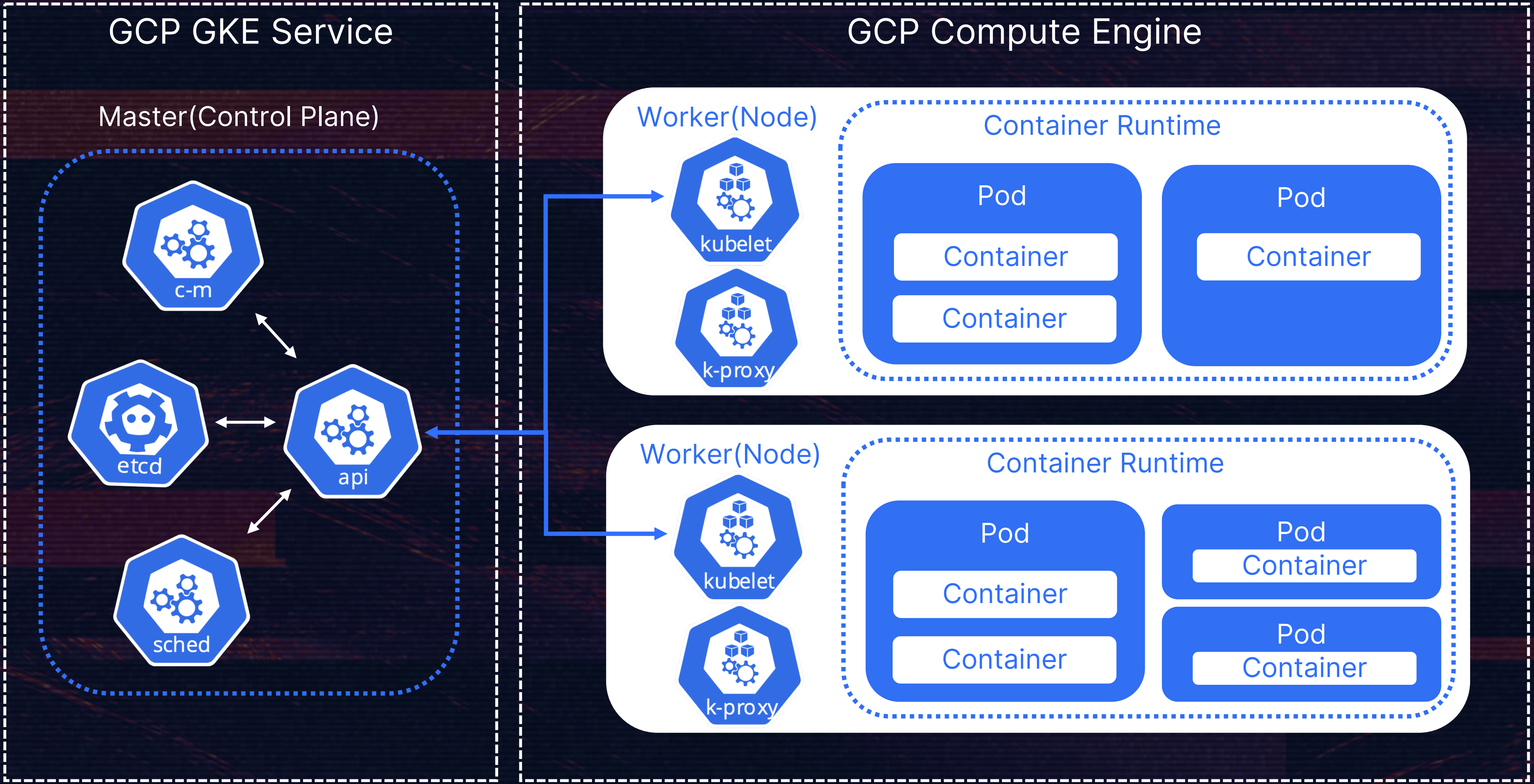
CYCRAFT

Kubernetes

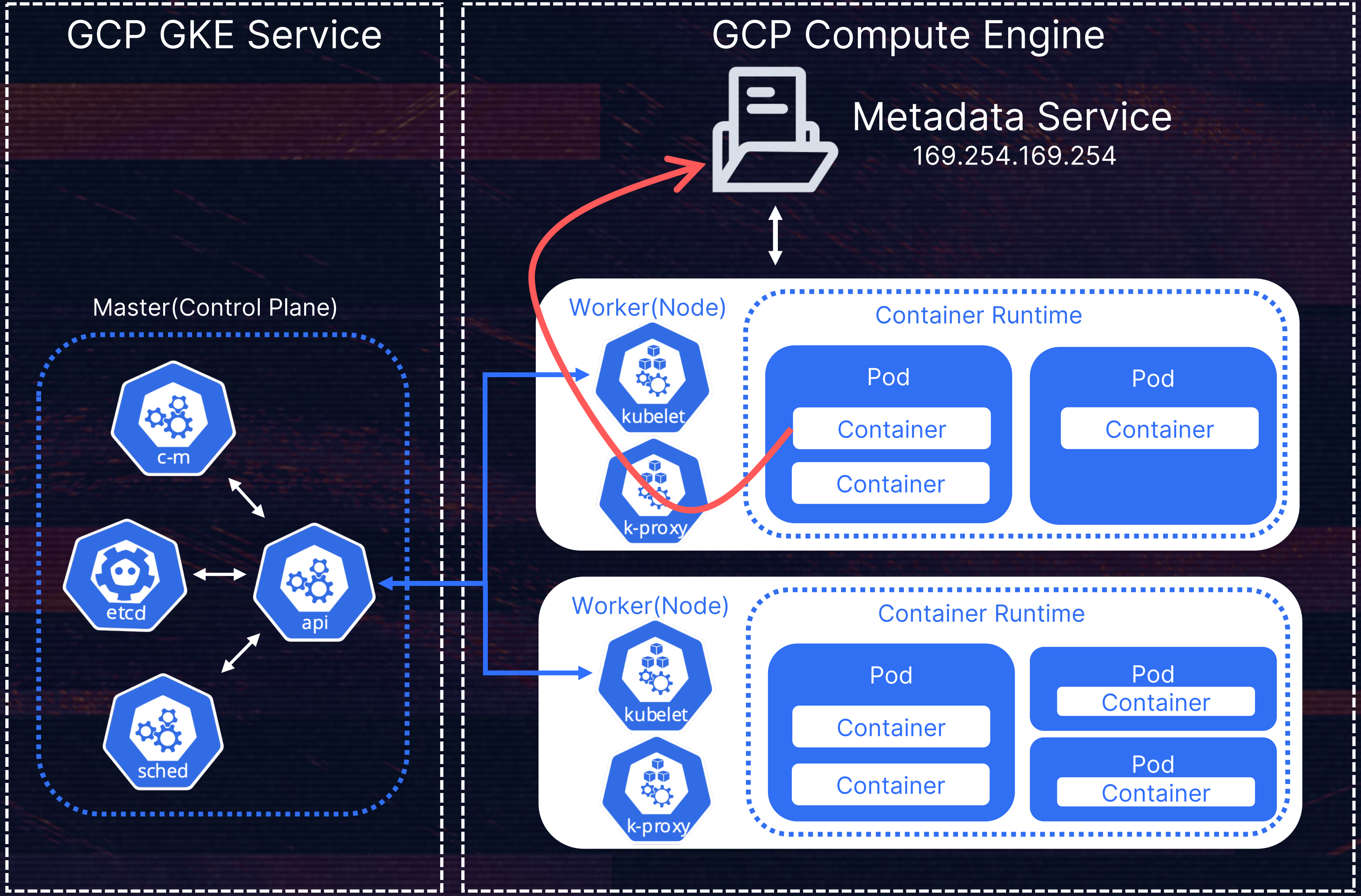


CYCRAFT

Kubernetes on GCP



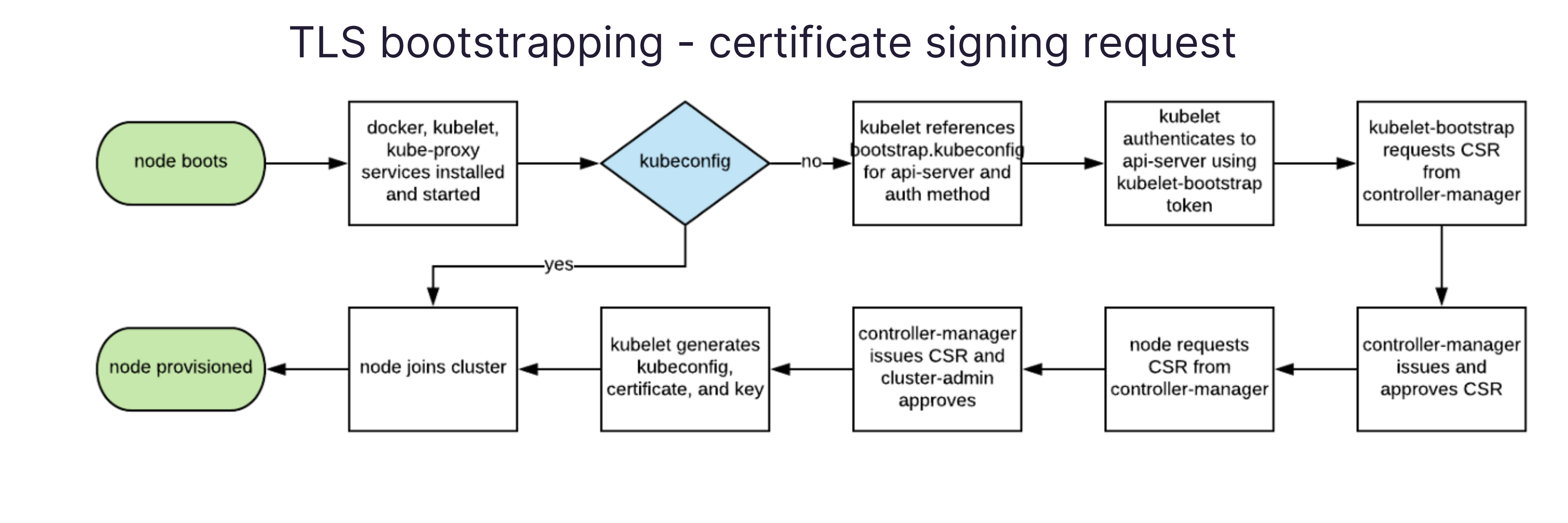
Instance Metadata Service?



CYCRAFT

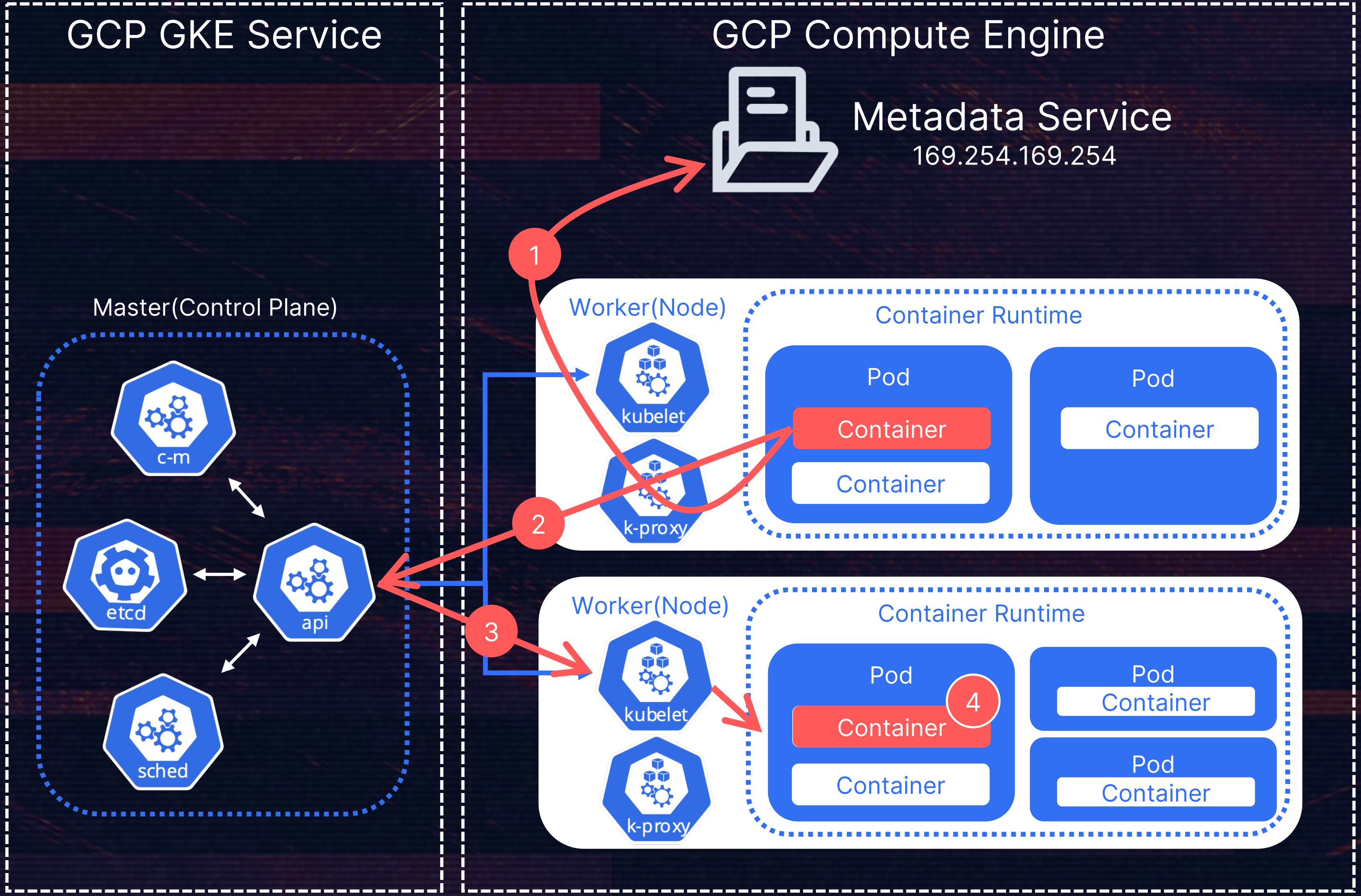
Secret in Metadata Service

- Kube-env
  - KUBELET_CERT
  - KUBELET_KEY


TLS bootstrapping - certificate signing request
node boots
docker, kubelet, kube-proxy services installed and started
kubeconfig
no
kubelet references bootstrap.kubeconfig for api-server and auth method
kubelet authenticates to api-server using kubelet-bootstrap token
kubelet-bootstrap requests CSR from controller-manager
controller-manager issues and approves CSR
node requests CSR from controller-manager
controller-manager issues CSR and cluster-admin approves
kubelet generates kubeconfig, certificate, and key
yes
node joins cluster
node provisioned

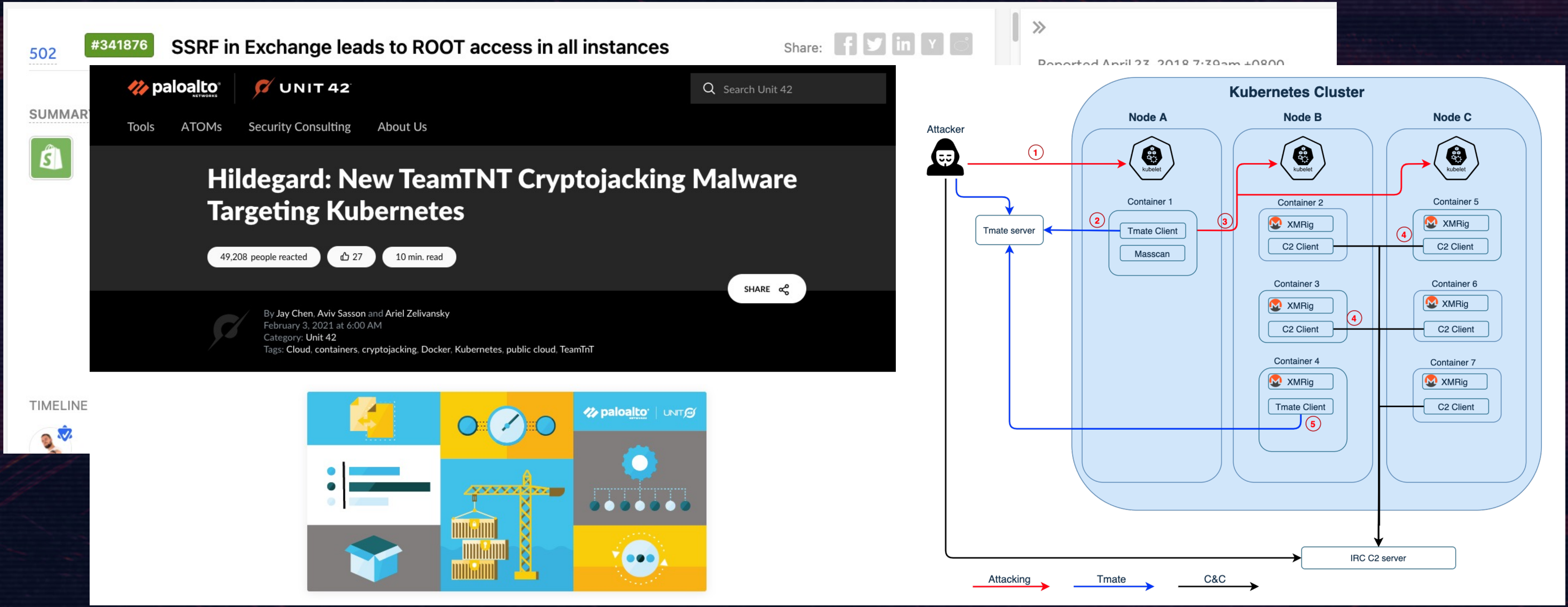
https://medium.com/@toddrosner/kubernetes-tls-bootstrapping-cf203776abc7

Instance Metadata Service?



CYCRAFT

Real World Case



502 #341876 SSRF in Exchange leads to ROOT access in all instances

Share:

SUMMAR

TIMELINE

Reported April 23, 2018 7:39am +0800

paloalto NETWORKS | UNIT 42

Search Unit 42

Tools ATOMs Security Consulting About Us

Hildegard: New TeamTNT Cryptojacking Malware Targeting Kubernetes

49,208 people reacted · 27 · 10 min. read

SHARE

By Jay Chen, Aviv Sasson and Ariel Zelivansky
February 3, 2021 at 6:00 AM
Category: Unit 42
Tags: Cloud, containers, cryptojacking, Docker, Kubernetes, public cloud, TeamTnT

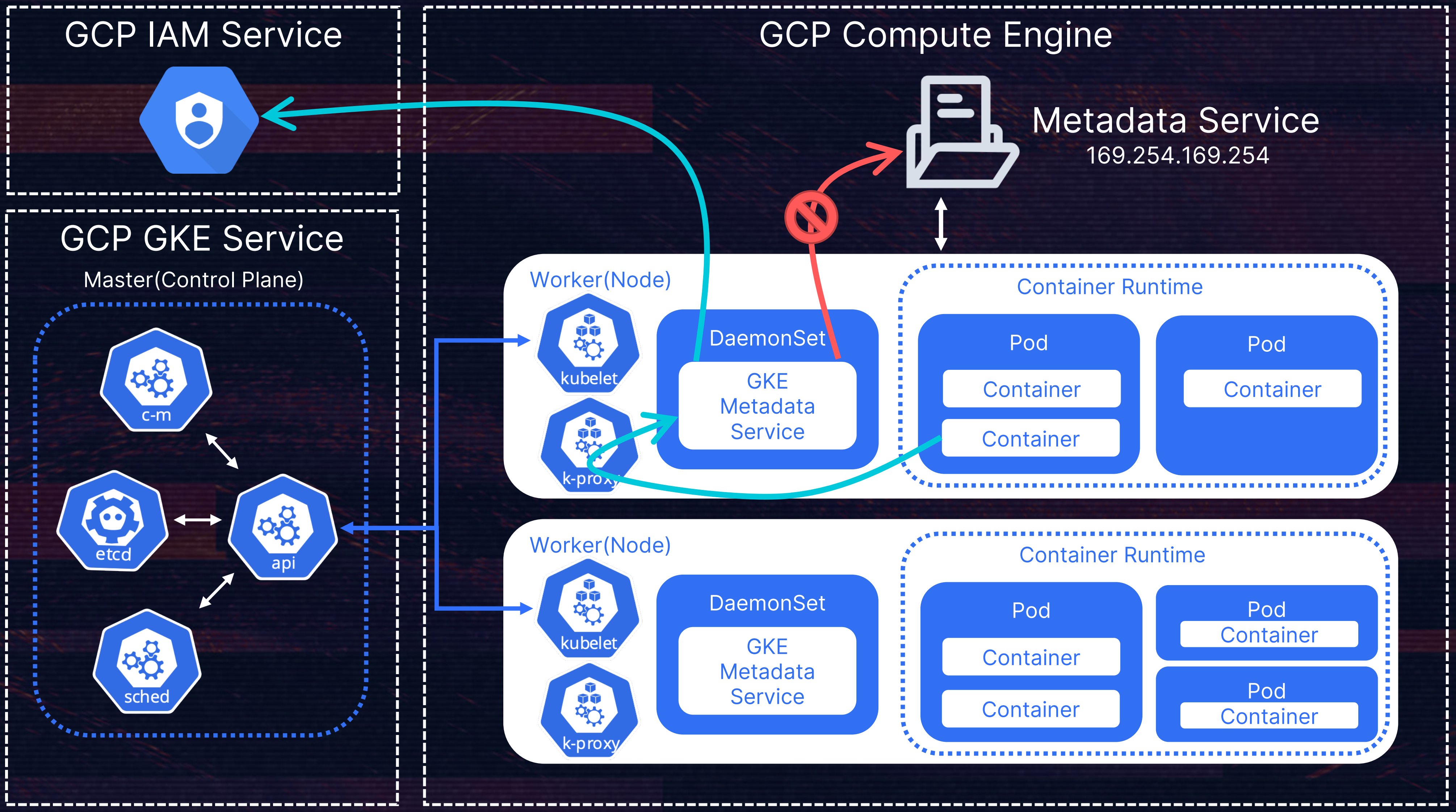
GCP 如何應對

- 目標：避免 Pods 取得 Bootstrap Credential
- Metadata concealment & Workload Identity
- Shielded GKE nodes

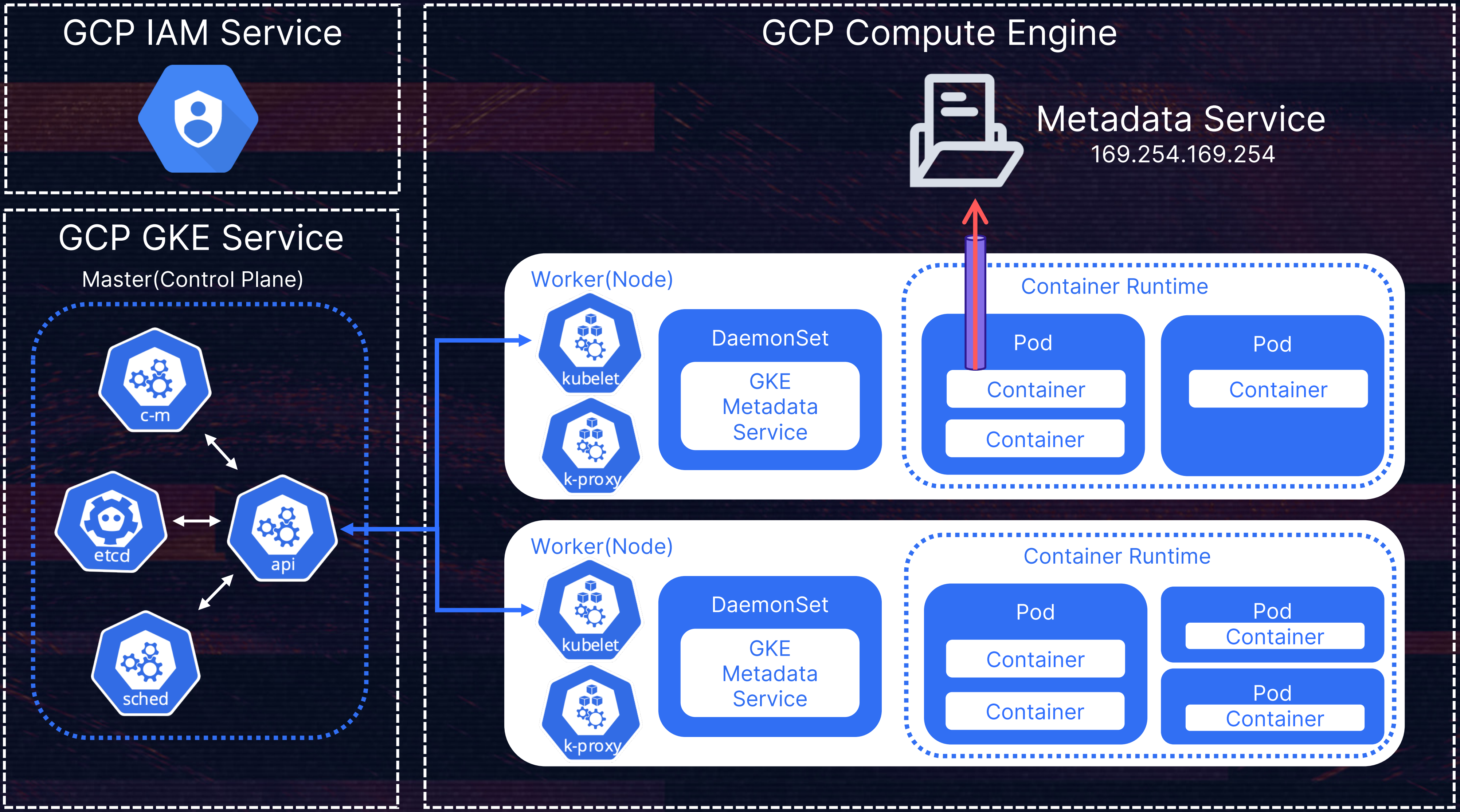
Metadata concealment & Workload Identity

- 目的：避免 Pods 直接與 Metadata Service 接觸
- 作法：攔截所有對 Metadata service 的請求
  - Metadata concealment：firewall
  - Workload Identity：proxy -> GKE metadata service

Workload Identity



Misconfig(Host Network) -> Bypass

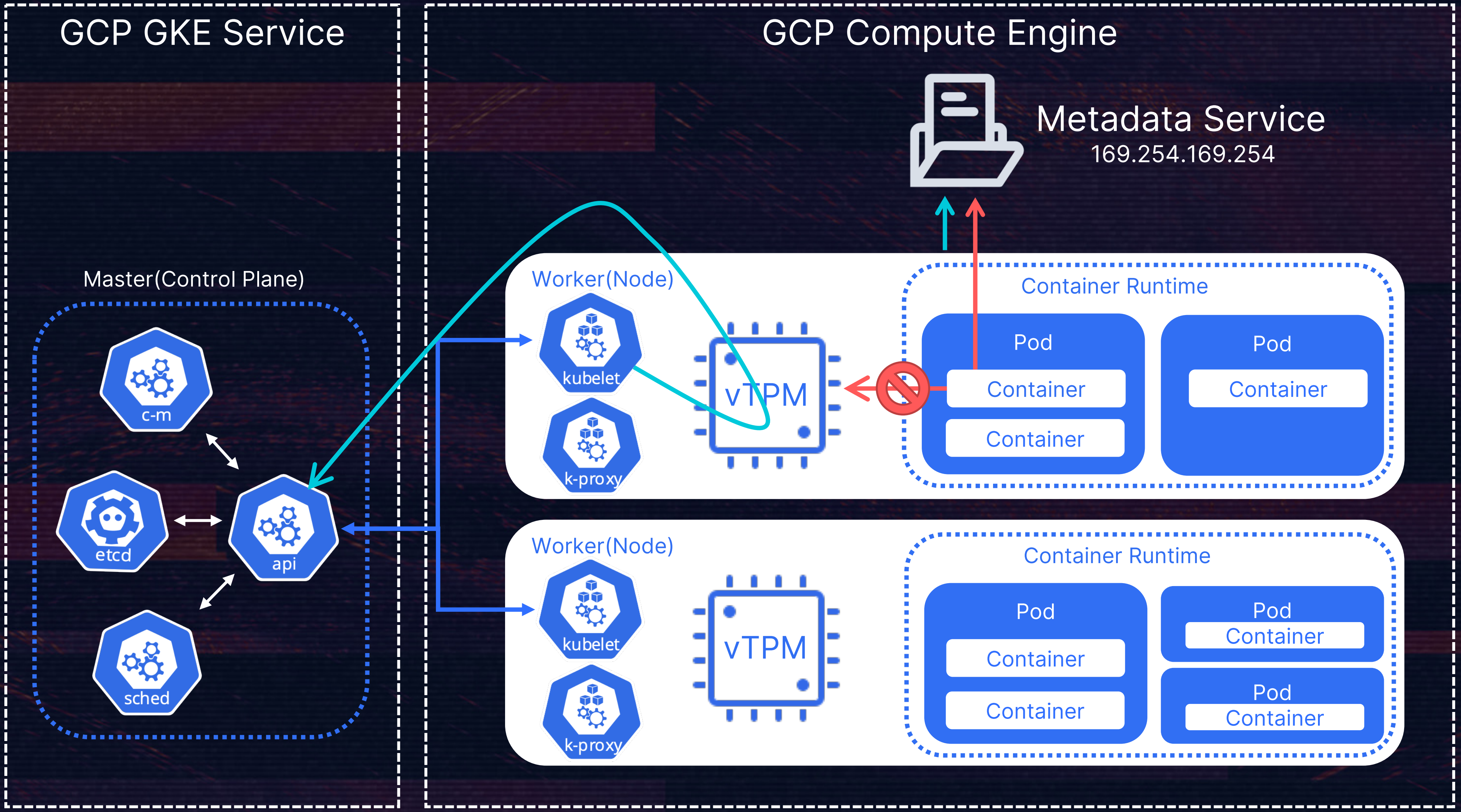


Shielded GKE nodes

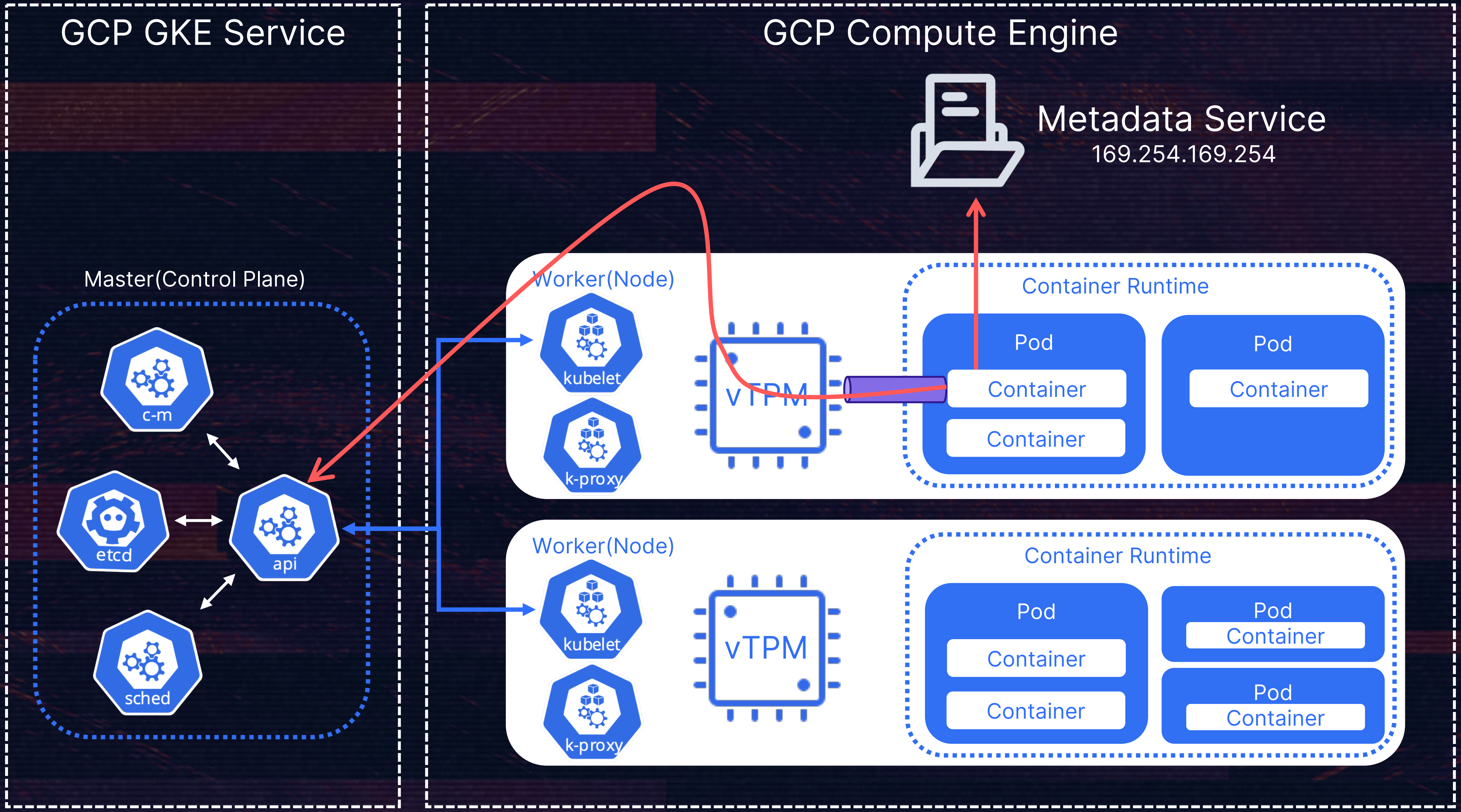
- Shielded VMs：用 vTPM 去驗證 VM 的完整性
  - 預防 rootkit、資料洩漏等
- 目的：區別 Worker(Node) 與 Pods
- 作法：做 certificate signing request 時，需要 vTPM 驗證
  - Worker(Node) 碰得到 vTPM
  - Pods 內的 Container 碰不到 vTPM

https://github.com/kubernetes/cloud-provider-gcp/blob/b3dec429d3fc06810cfc5ef7aa493efdcac9fe6d/cmd/gke-exec-auth-plugin/tpm.go#L82

Shielded GKE nodes



Misconfig(privileged) -> Bypass



CYCRAFT

Defense

>如對藍隊工具整理感興趣，請來信索取

>dange.lin@cycarrier.com