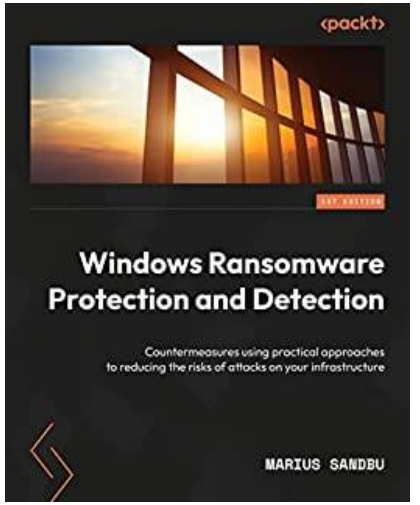
Kubernetes + Security = True?

Or...maintaining high velocity and still wearing a seatbelt

WHOAMI$

- **Cloud Evangelist – Sopra Steri**
- **Focus areas**: **Cloud & Security**
- **«Hobbies»**
  - Microsoft Cloud Security User Group
  - Cloudfirst Podcast
  - Tech influencer msandbu.org
  - Also an author sometimes



Microsoft Security User Group Norway

C2 - Restricted

©2022 Microsoft Security User Group Norway All Rights Reserved

github.com/msugn
@MsSecUGNorway
#MSUGN

What is the biggest challenge with securing Kubernetes?

The biggest challenge with securing Kubernetes is the complex and dynamic nature of the environment. Kubernetes is a highly distributed system that consists of multiple components and layers making it inherently more difficult to secure compared to traditional monolithic architectures. Here are some key challenges:

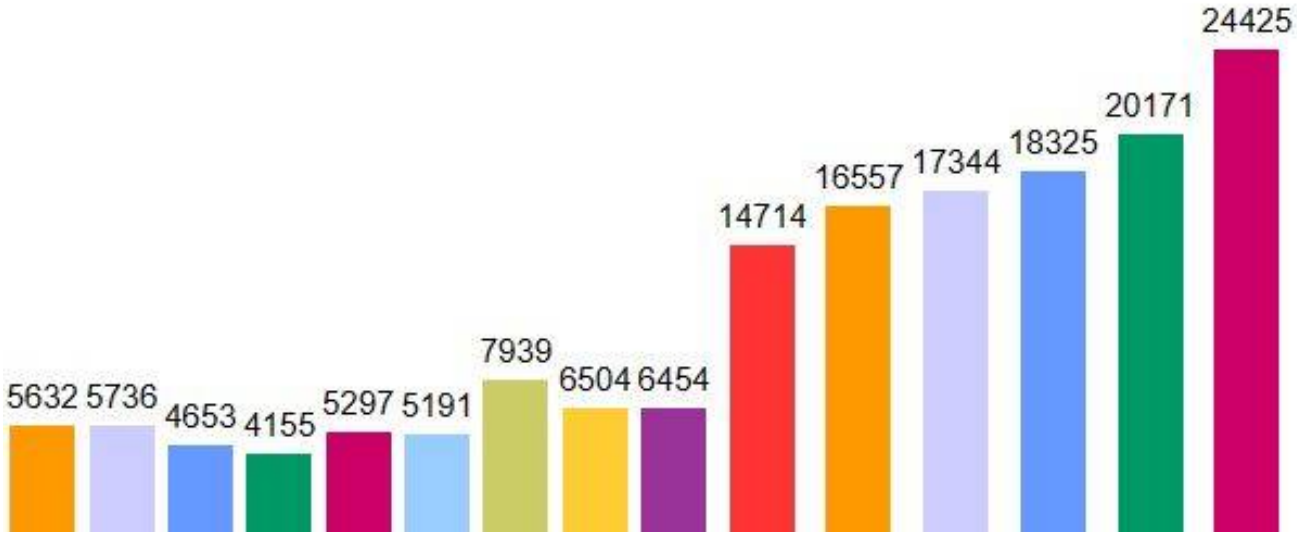
C2 - Restricted
©2022 Microsoft Security User Group Norway All Rights Reserved

From the NSM Risk report 2023

Utnyttelse av cybersårbarheter lar ikke vente på seg

I Norge har vi fra 2019 til 2021 sett en tredobling i alvorlige cyberoperasjoner mot norske myndig-heter og virksomheter. Antallet alvorlige og svært

50.000 norske kroner i tapt inntekt per minutt – det er scenariet for foretak som opplever feil som gjør digitale tjenester utilgjengelige for kundene.



The number of vulnerabilities from 2008 – 2022

©2022 Microsoft Security User Group Norway All Rights Reserved

Attack vectors

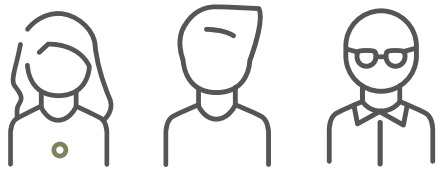
IT

Collaboration

Physical access

Email

Web



Developers

Vulnerabilities

Misconfigured Services

DDoS-/DoS-attacks

User information hijacked

Phishing

Drive-by download

Vulnerabilities in external services

Public exposed services

TCP SYN Flood / HTTP GET/POST Flood

Credential Stuffing – MFA Fatigue / Access tokens

Qbot / Icedid

RedLineStealer / Vidar

Microsoft Security User Group Norway

C2 - Restricted

©2022 Microsoft Security User Group Norway All Rights Reserved

github.com/msugn

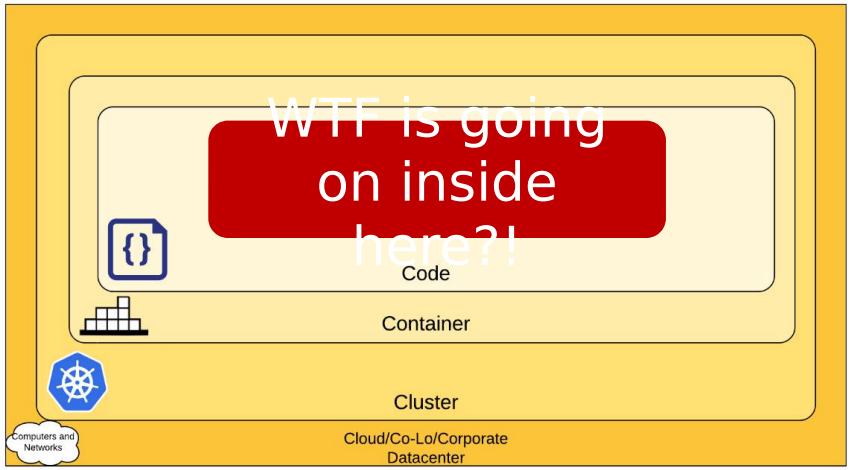
@MsSecUGNorway

#MSUGN

Risks in a Cloud-native landscape?

- Unauthorized access to Kube API
- Unauthorized access to CI/CD and sourcecode
- Vulnerabilities in Container Image or source code
- Limited to none network «segmentation» policies
- Harvested user credentials/tokens/SPNs
- Credentials stored in plaintext in container

Container applications



The 4C's of Cloud Native Security

- Vulnerabilities in Kubernetes
- Container Escape
- Supply-chain vulnerabilities
- Limited network insight
- Limited security control of container registry
- No proper RBAC in place

[Tactics - Threat Matrix for Kubernetes https://microsoft.github.io/Threat-Matrix-for-Kubernetes/](https://microsoft.github.io/Threat-Matrix-for-Kubernetes/)

Microsoft Security User Group Norway

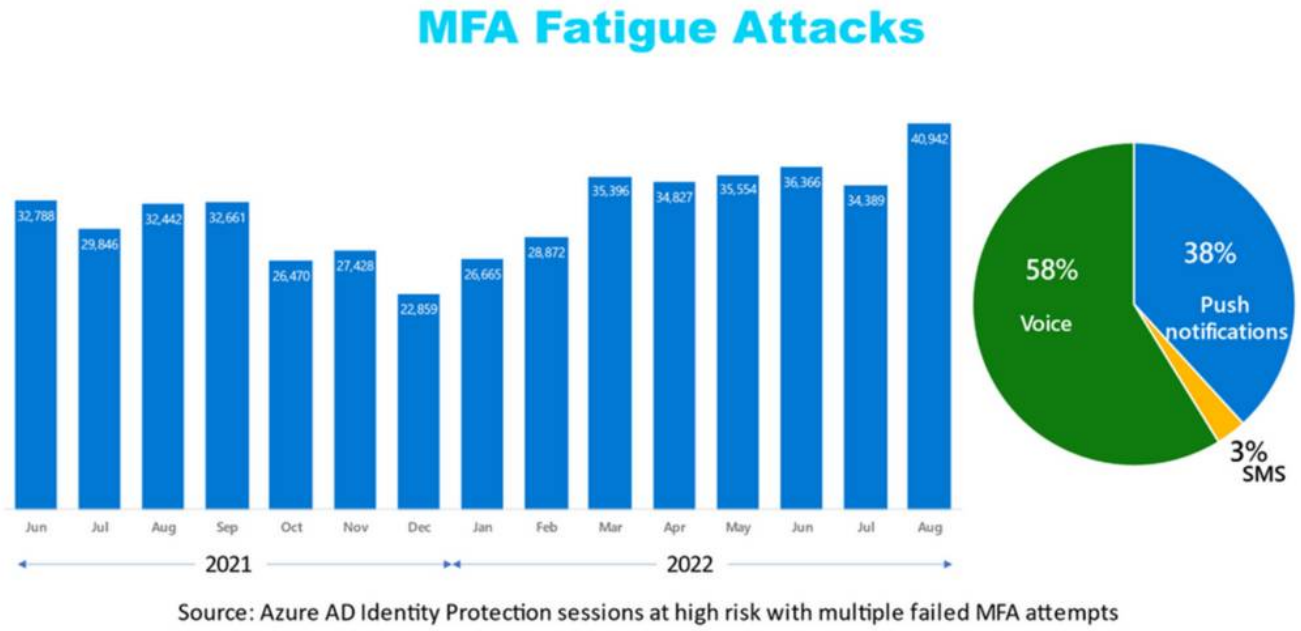
C2 - Restricted

©2022 Microsoft Security User Group Norway All Rights Reserved

github.com/msugn
@MsSecUGNorway
#MSUGN

Identity also a much bigger challenge

300% Increase in identity-based attacks the last



Source: Azure AD Identity Protection sessions at high risk with multiple failed MFA attempts

Hackers Breached Colonial Pipeline Using Compromised Password

- Investigators suspect hackers got password from dark web leak
- Colonial CEO hopes U.S. goes after criminal hackers abroad

Uber suffers major cyber attack

Details are trickling out of an apparent 'near total' compromise of ride-sharing service Uber by an alleged teenage hacktivist

Reusing username and passwords on different sites

Phishing attacks and credential harvesting

MFA Fatigue attacks

Microsoft Security User Group Norway

C2 Restricted

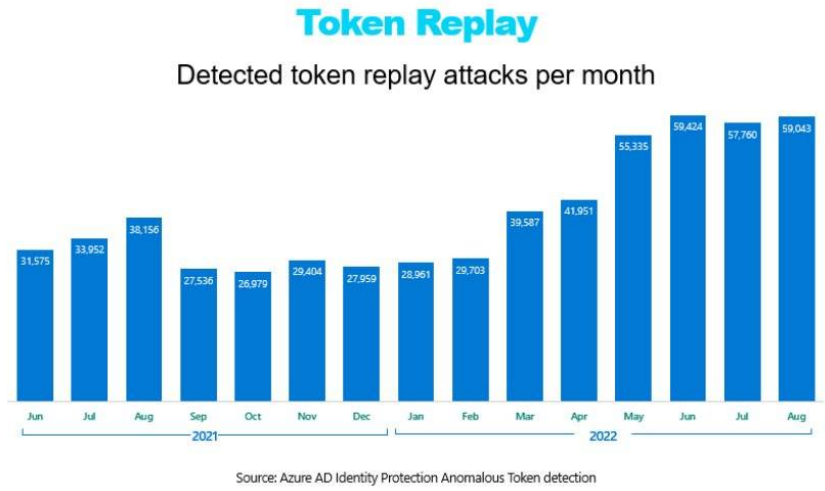
©2022 Microsoft Security User Group Norway All Rights Reserved

github.com/msugn
@MsSecUGNorway
#MSUGN

What other security threats?

Post-authentication attacks

Determined attackers are using malware to steal tokens from devices—allowing a valid user to perform valid multifactor authentication on a valid machine, but then using credential stealers to take the cookies and tokens and use them elsewhere. This method is on the rise and has been used in recent high-profile attacks. Tokens can also be stolen if incorrectly logged or if intercepted by compromised routing infrastructure, but the most common mechanism by far is malware on a machine. If a user is running as admin on a machine, then they are just one click away from token theft. Core Zero Trust principles like running effective endpoint protection, managing devices, and, critically, using least privileged access (meaning, run as a user, not an admin, on your machines) are great defenses. Pay attention to signals that indicate that token theft is occurring, and require re-authentication for critical scenarios like machine enrollment.



Analysis of 4 Million Docker Images Shows Half Have Critical Vulnerabilities

Snyk finds 200+ malicious npm packages, including Cobalt Strike dependency confusion attacks

State of Kubernetes Security Report 2022

State of Open Source Security Report 2022

Microsoft Security User Group Norway
C2 - Restricted
©2022 Microsoft Security User Group Norway All Rights Reserved

Kubernetes (k8s) Architecture

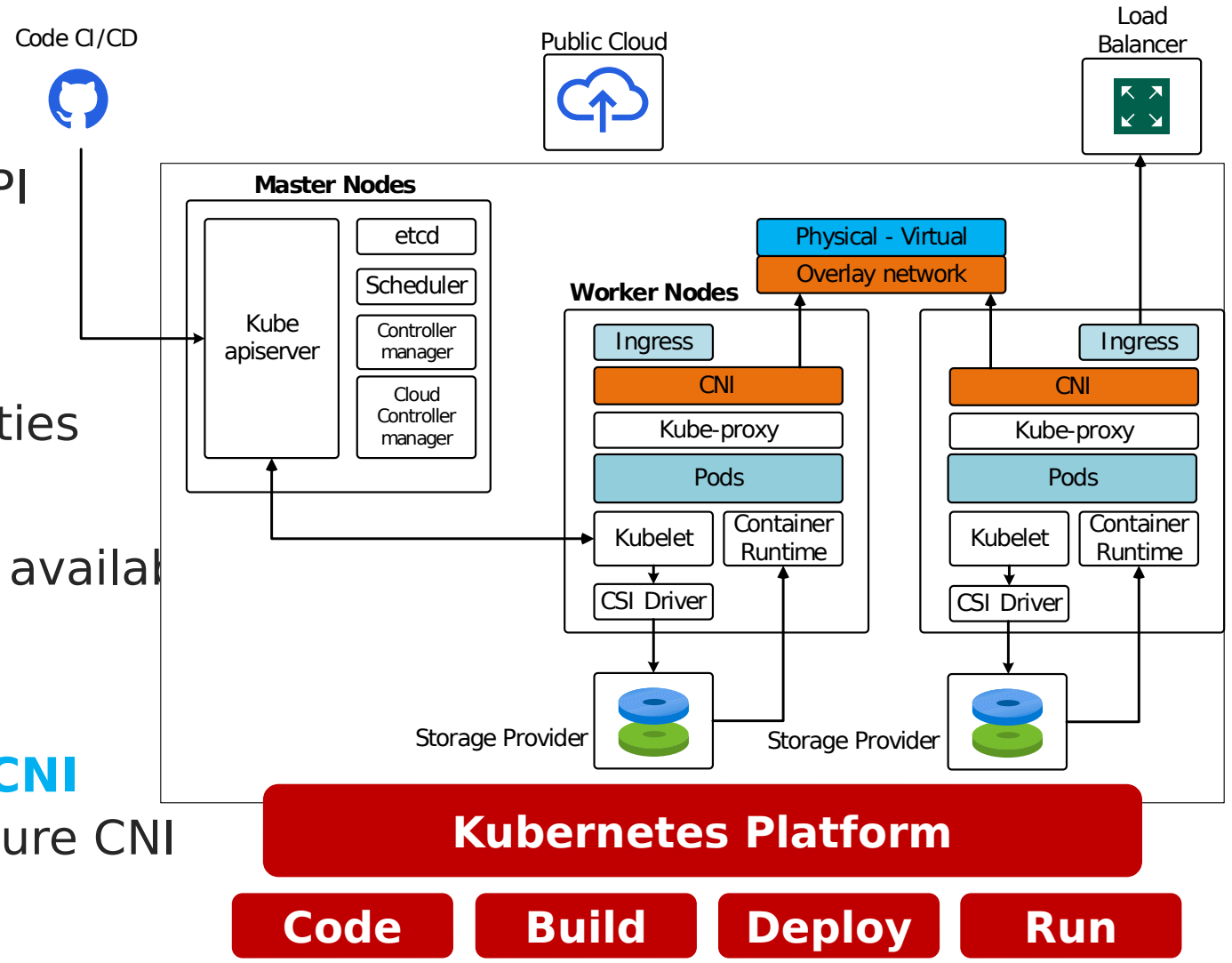
Integrations will differ

- **CSI** = Storage and Secrets
- **Cloud Controller Manager** = API integration to cloud providers
- **Load Balancer and Ingress**
- **Windows** **and** **Linux** nodes
- A huge ecosystem with oppurtunities

Often many security mechanisms availab from the providers

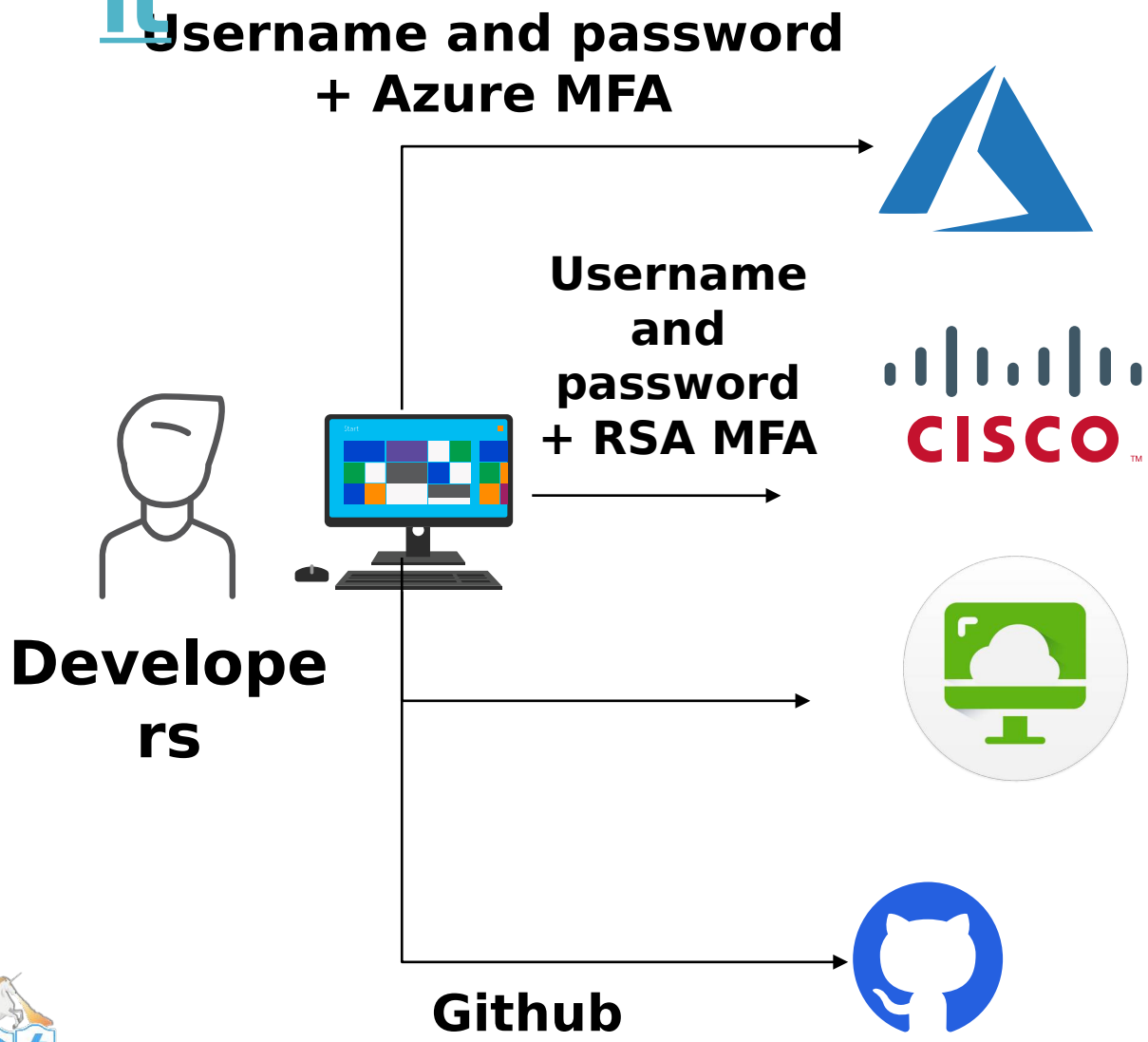
Network uses an integration called **CNI**

- Example: Cilium, VMware NSX, Azure CNI



©2022 Microsoft Security User Group Norway All Rights Reserved

Real-life scenario on how you shouldn't do it



Access internal services using VDI

NO healthcheck of device

Multiple agents and MFA services

No MFA on the github account (at that time)

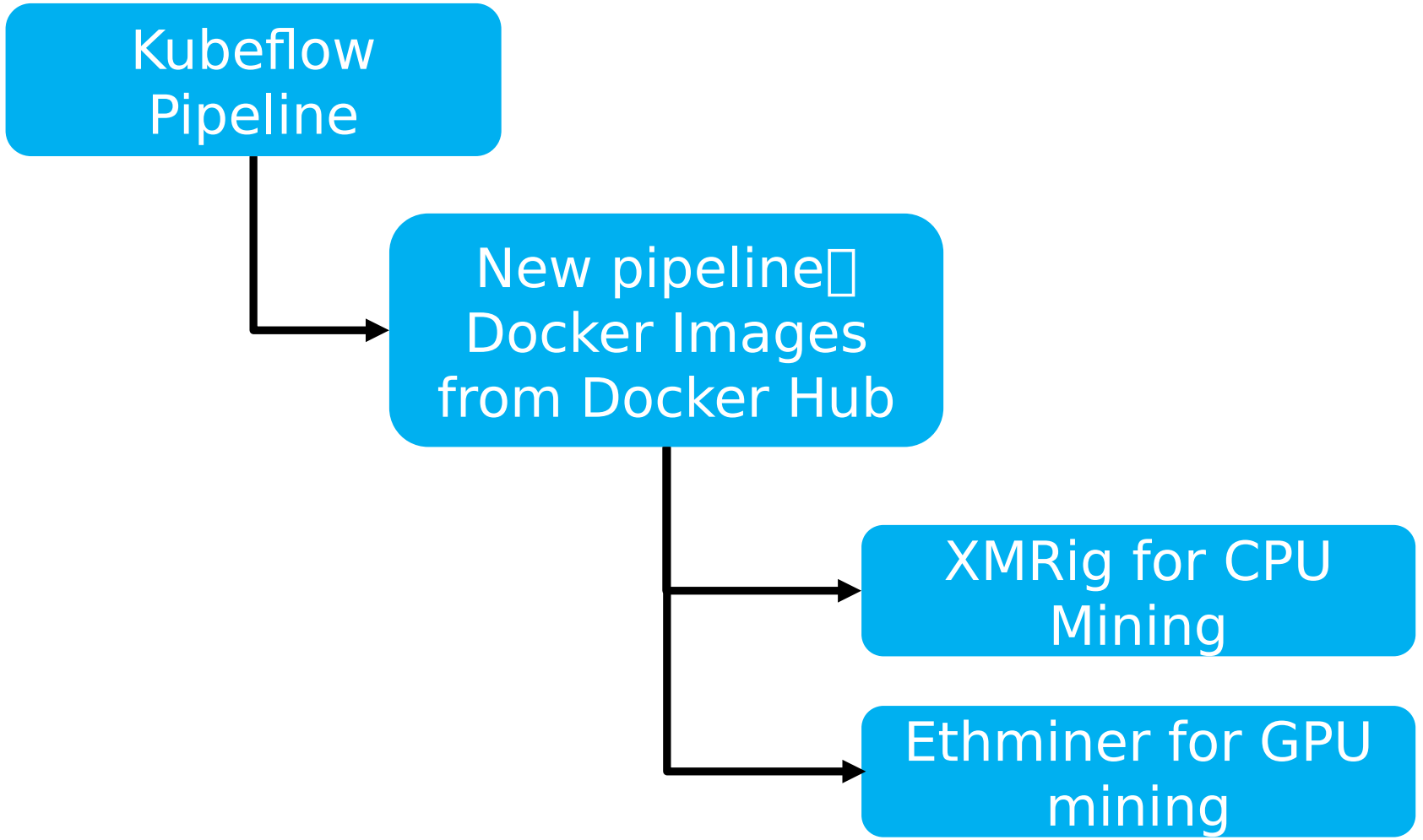
©2022 Microsoft Security User Group Norway All Rights Reserved

Not all attacks are that critical (but they can be!)

Kubernetes with Kubeflow

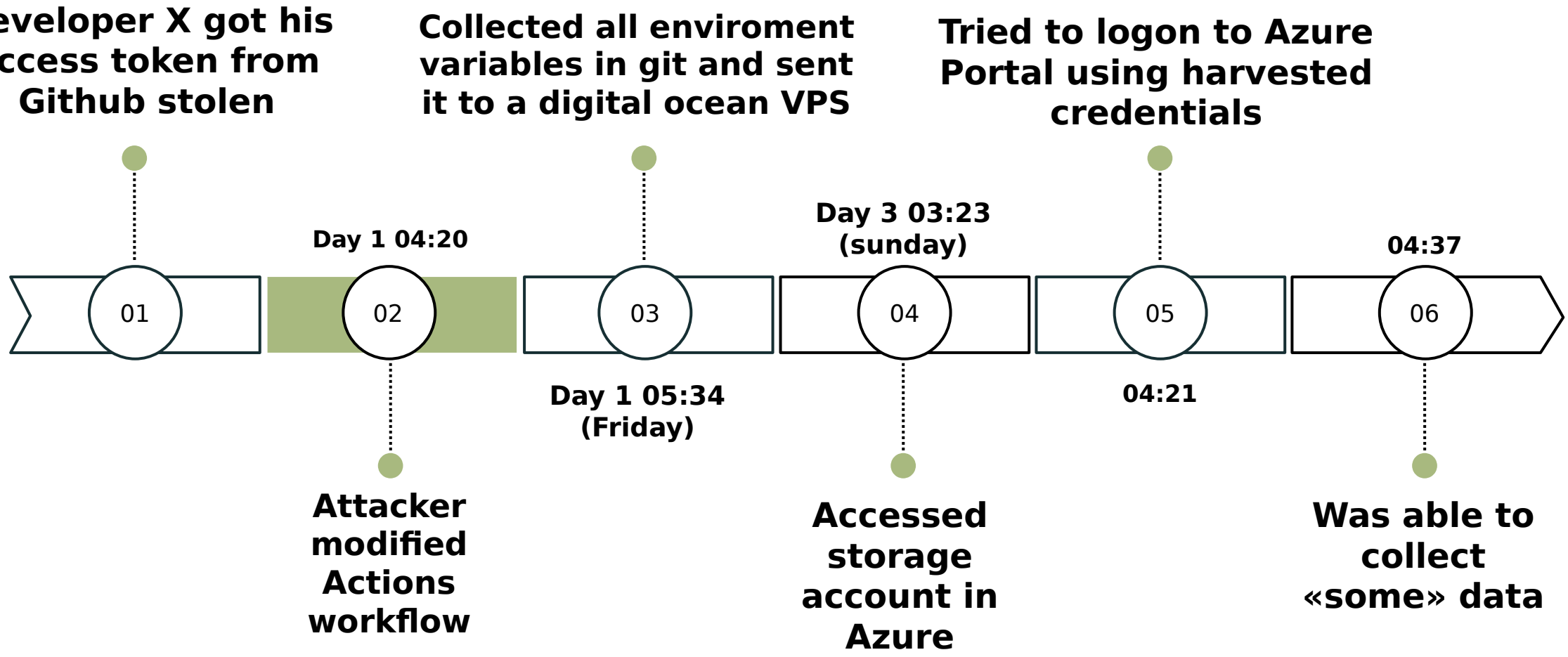
Using Kubeflow to trigger Tensor flow jobs

Kubeflow dashboard open to internet



©2022 Microsoft Security User Group Norway All Rights Reserved

Compromised Git pipeline

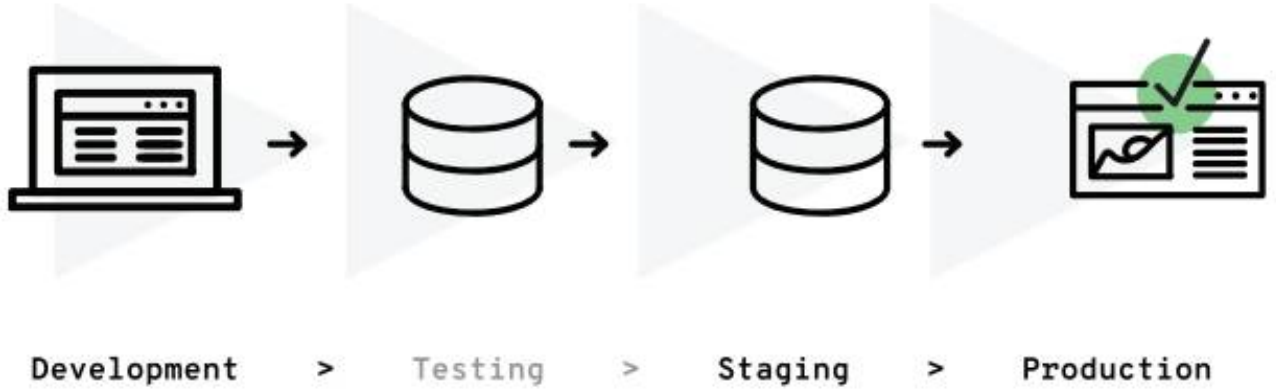


Microsoft Security User Group Norway
C2 - Restricted
©2022 Microsoft Security User Group Norway All Rights Reserved

github.com/msugn
@MsSecUGNorway
#MSUGN

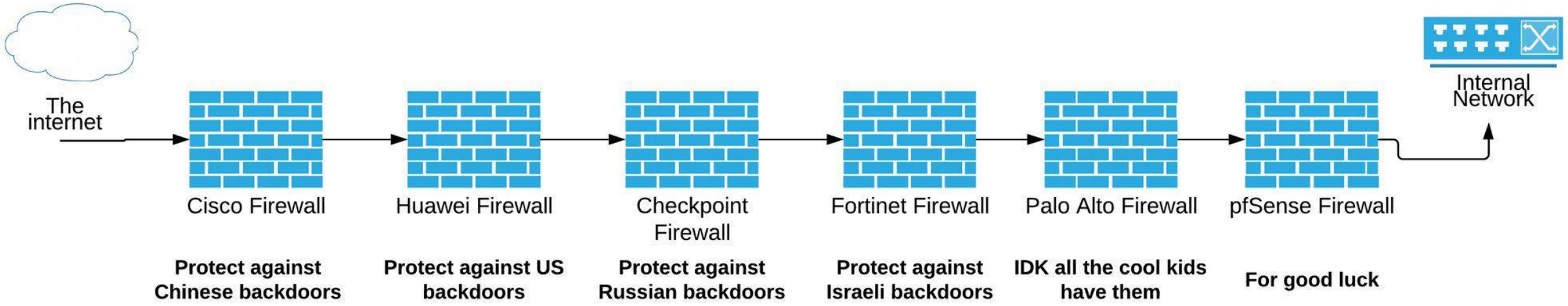
What kind of countermeasures can we implement?

Not one size fits all – Some mechanisms are entirely **depedant on use-case** and security requirements of an organization



©2022 Microsoft Security User Group Norway All Rights Reserved

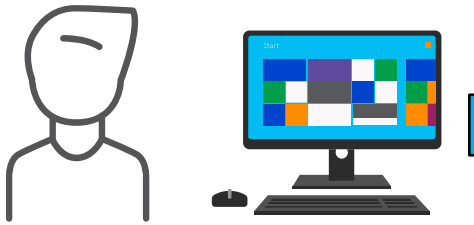
Securing the developer experience



©2022 Microsoft Security User Group Norway All Rights Reserved

Zero-Trust Network Access

Never Trust
Always Verify



End-user

Identity Posture

Device Posture

ZTNA Magic

Condition based access

Lokasjon | **Tidspunkt**

Data | **Session**

SaaS
TCP/UDP
Web Apps
Windows Apps
File Storage
Jumphost

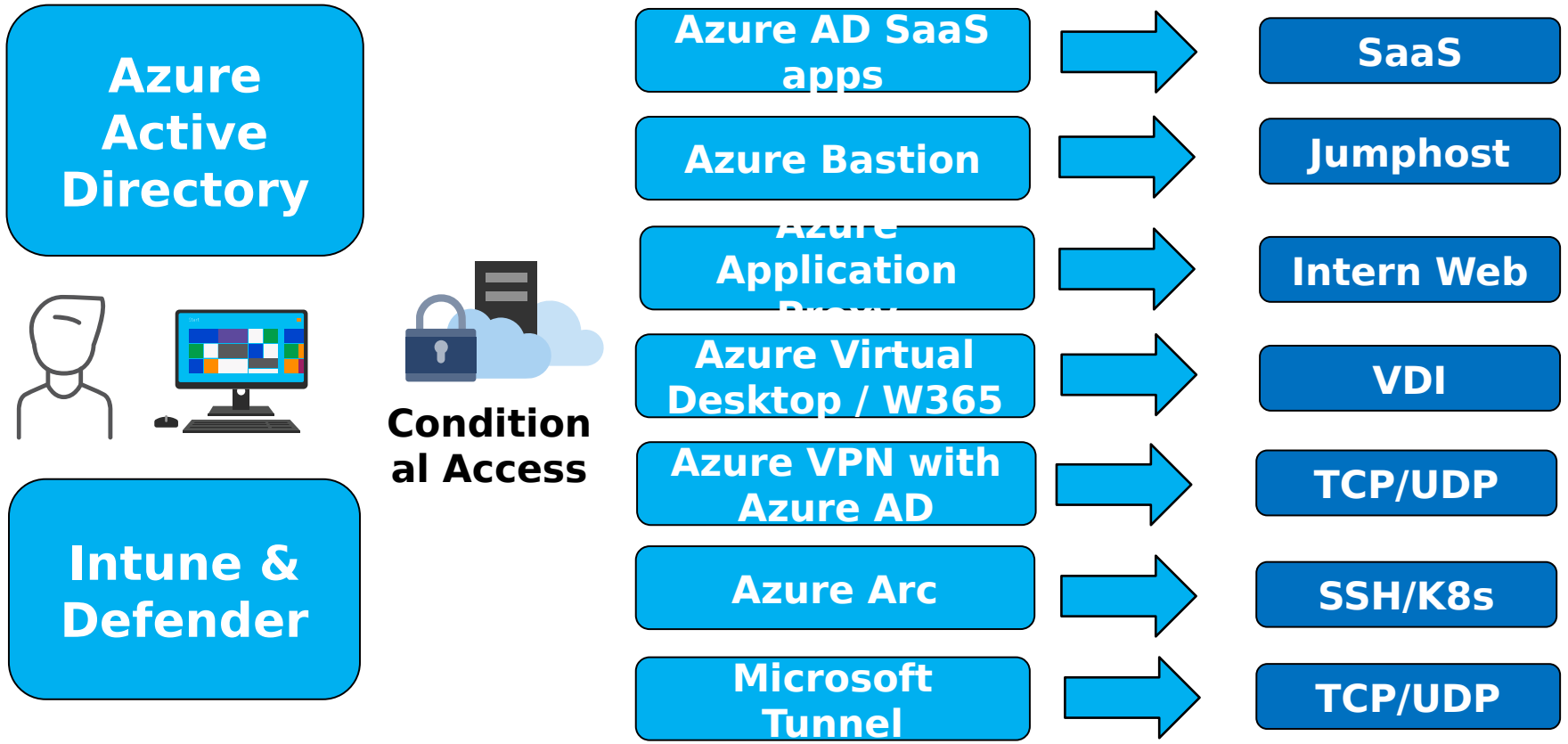
Microsoft Security User Group Norway

C2 - Restricted

©2022 Microsoft Security User Group Norway All Rights Reserved

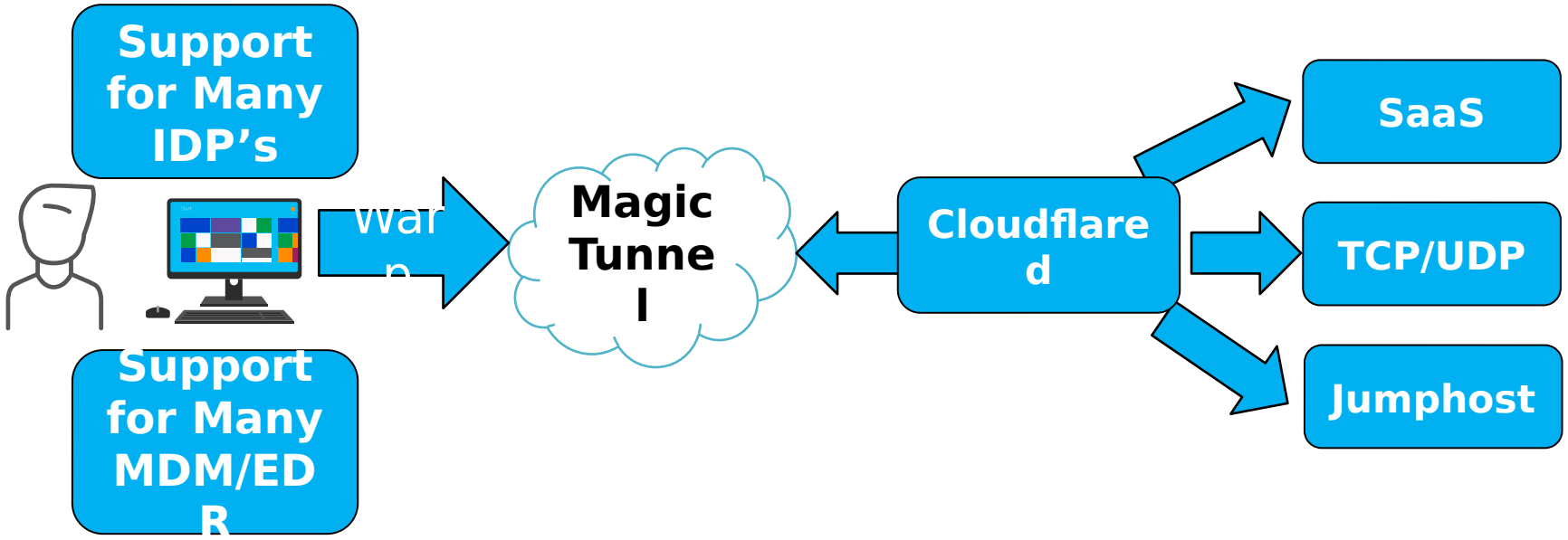
github.com/msugn
@MsSecUGNorway
#MSUGN

Microsoft’s approach



©2022 Microsoft Security User Group Norway All Rights Reserved

Cloudflare Zero-Trust



C2 - Restricted

©2022 Microsoft Security User Group Norway All Rights Reserved

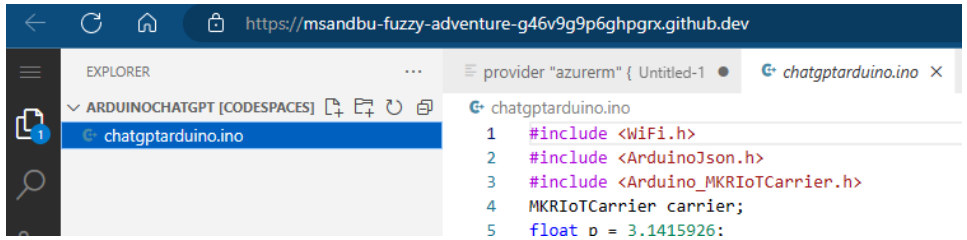
Securing the developer workbench

VS Code – Local development

GitPod

Github Codespaces

Provide non-persistent container, web-based
Deployed as isolated pod
As SaaS service can integrate with CASB
Allow use of central iDP



Virtual Desktop

For workloads not supported in web-IDE
Example: Hardware development (Custom drivers)
Provide secure virtual desktop with locked down OS

©2022 Microsoft Security User Group Norway All Rights Reserved

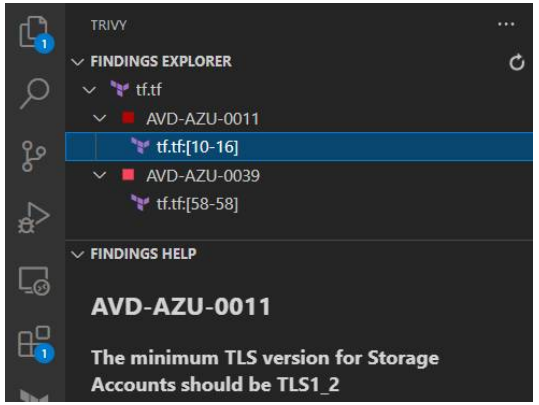
Securing the developer workbench – Extensions!

Be Careful of which extenions you use!

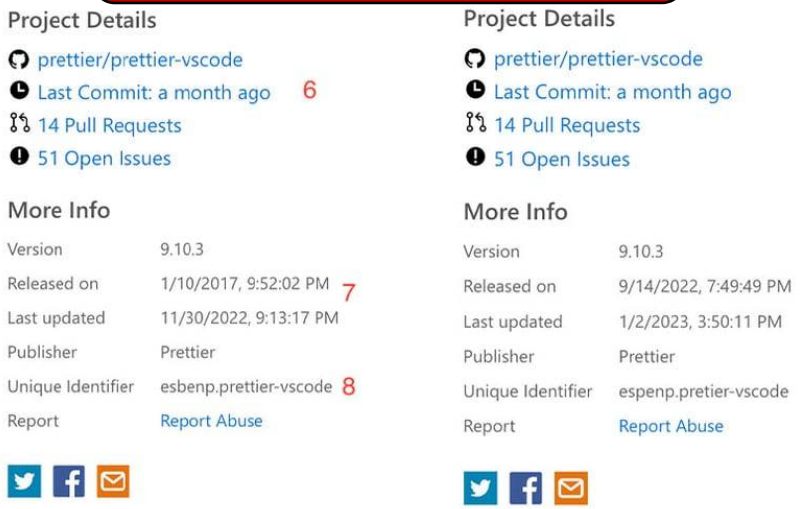
- Double check publisher
- Double check released date

Some useful extensions for code analys

- Checkov (Palo Alto – Requires Prism Cloud API)
- Trivy (Requires API access to Aqua Security)
- Tfsec (Full open source)
- Snyk (Requires API access to Snyk.io)



Can you spot the fake one?



Also be careful with Copilot

```
os_profile {
  computer_name  = "example-vm"
  admin_username = "adminuser"
  admin_password = "Password1234!"
}

os_profile_linux_config {
  disable_password_authentication = false
}
```

Microsoft Security User Group Norway

C2 Restricted

©2022 Microsoft Security User Group Norway All Rights Reserved

msugn
@MsSecUGNorway
#MSUGN

Security mechanisms for GitHub

SCIM – User provisioning from central iDP

SSO and access management using **SAML/OA**

Self-hosted runners and private repositories

Provide the ability to control and restrict the traffic flow

TFSec = Inspect security issues in Terraform c

Trivy = Inspect security issues in TF Code and Container images

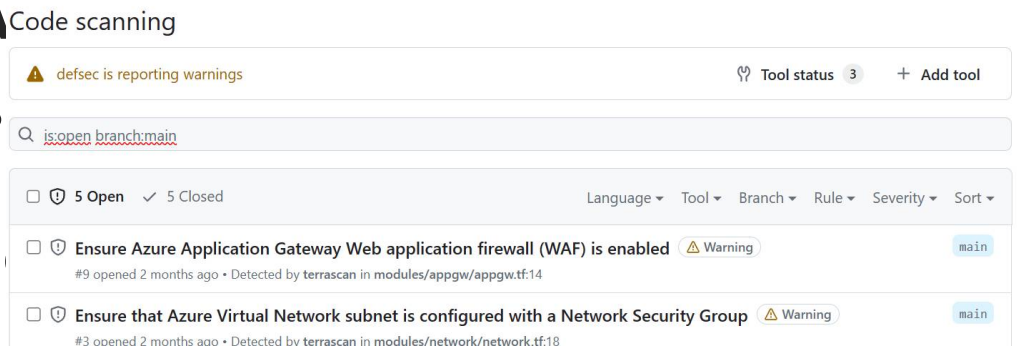
Git Signed Commit

Github Advanced Security

Secret scanning = Free feature

Manage programatic access

Use of fine-grained personal access tokens



Github Advanced Security: (features for private repositories)

Code scanning
Secret Scanning
Depedency Review

Microsoft Security User Group Norway

C2 - Restricted

©2022 Microsoft Security User Group Norway All Rights Reserved

github.com/msugn
@MsSecUGNorway
#MSUGN

IAM mechanisms and RBAC

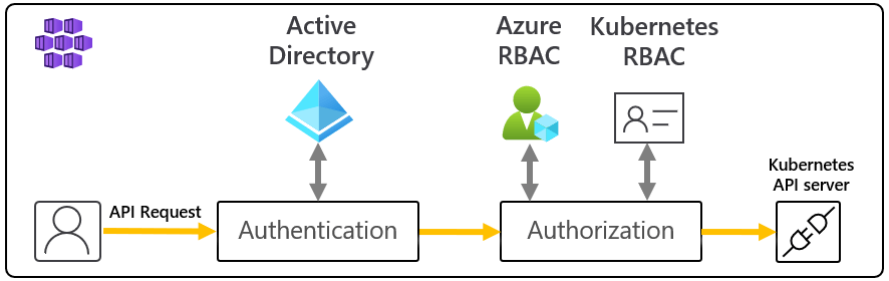
Accessing Kubernetes API trough

Token, **Sertifikat** or **authentication proxy**

Built-in Certificate in Kubernetes cannot be revoke

No standard LDAP integration

dexidp/dex or pinniped



Example: **Azure AD, Google** or **OpenID Connect**

RBAC is only to add permissions no deny mechanism

Roles can be defined on namespace level or clust

```
apiVersion:
rbac.authorization.k8s.io/v1
kind: Role
metadata:
namespace: default
name: pod-reader
rules: - apiGroups: [""] # ""
resources: ["pods"]
 verbs: ["get", "watch", "list"]
```

```
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
name: read-pods
 namespace: default
subjects:
 - kind: User
name: minikube
apiGroup: rbac.authorization.k8s.io
roleRef: kind:
Role name: pod-reader
apiGroup: rbac.authorization.k8s.io
```

RBAC and API Objects
All permissions can be delegated(CRUD)

Role **Rolebinding** **Namespace**

ClusterRol e **ClusterRoleBinding**

sighupio/permission-manager

Microsoft Security User Group Norway

C2 - Restricted

©2022 Microsoft Security User Group Norway All Rights Reserved

github.com/msugn
@MsSecUGNorway
#MSUGN

Private Cluster

No limit on authentication requests

Mostly an issue on Kubernetes in Public Cloud

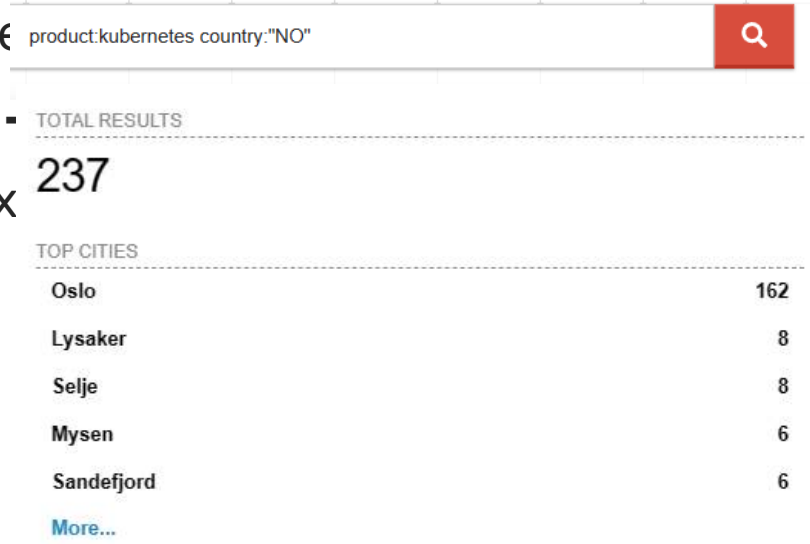
Redusere abuse of tokens or other credentials against Kube

A few vulnerabilites here the last years (example: **CVE-2022-**

.....or atleast define authorized IP addresses for Kube-API prox

Reconfigure to Private Cluster will often require a redeployment of the cluster

Shodan check today!



©2022 Microsoft Security User Group Norway All Rights Reserved

Is it according to best pratices?

Kubebench – Scans enviroment according to CIS

Kubescape – Scans enviroment according to NSA-CISA and CIS

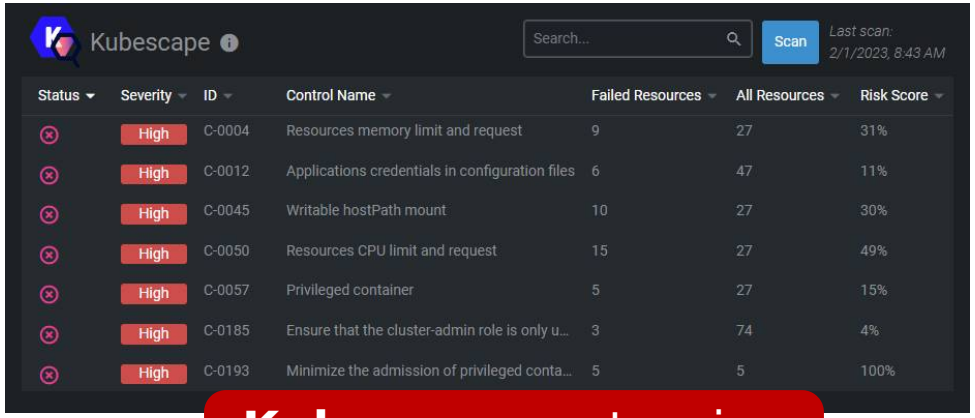
Both understand limitations when running in Microsoft Azure

Kubescape can also run using Github Actions or CLI

YAML or JSON based reporting

```
Controls: 22 (Failed: 2, Excluded: 13, Skipped: 2)
Failed Resources by Severity: Critical – 0, High – 0, Medium – 24, Low – 0

+----------+-----------------------------------------+------------------+--------------------+-----------------+---------------+
| SEVERITY |                CONTROL NAME             | FAILED RESOURCES | EXCLUDED RESOURCES | ALL RESOURCES | % RISK-SCORE |
+----------+-----------------------------------------+------------------+--------------------+-----------------+---------------+
| Critical | Disable anonymous access to Kubelet service |        0         |         0          |        0        |    skipped*   |
| Critical | Enforce Kubelet client TLS authentication |        0         |         0          |        0        |    skipped*   |
| High     | Resource limits                         |        0         |         7          |       19        |       0%      |
| High     | HostNetwork access                      |        0         |         6          |       19        |       0%      |
| High     | Privileged container                    |        0         |         1          |       19        |       0%      |
| Medium   | Exec into container                     |        0         |         2          |       70        |       0%      |
| Medium   | Non-root containers                     |        0         |         7          |       19        |       0%      |
| Medium   | Allow privilege escalation              |        0         |         6          |       19        |       0%      |
| Medium   | Ingress and Egress blocked              |        12        |         7          |       19        |      63%      |
| Medium   | Automatic mapping of service account    |        12        |         46         |       58        |      21%      |
| Medium   | Cluster-admin binding                   |        0         |         2          |       70        |       0%      |
| Medium   | Cluster internal networking             |        0         |         4          |        4        |       0%      |
| Medium   | Linux hardening                         |        0         |         2          |       19        |       0%      |
| Medium   | Secret/ETCD encryption enabled          |        0         |         1          |        1        |       0%      |
| Medium   | Audit logs enabled                      |        0         |         1          |        1        |       0%      |
| Low      | Immutable container filesystem          |        0         |         6          |       19        |       0%      |
| Low      | PSP enabled                             |        0         |         1          |        1        |       0%      |
+----------+-----------------------------------------+------------------+--------------------+-----------------+---------------+
|          |              RESOURCE SUMMARY          |        12        |         52         |       143       |     5.48%     |
+----------+-----------------------------------------+------------------+--------------------+-----------------+---------------+
```



Kubescape extension for Lens / Openlens

Microsoft Security User Group Norway

C2 - Restricted

©2022 Microsoft Security User Group Norway All Rights Reserved

github.com/msugn

@MsSecUGNorway

#MSUGN

Upgrades and patching

1 year support on a minor release

Version now 1.26.1 (major.minor.patc

Maintance for 14 months

Some different standards on what is suppo

Depending on vendor

Kubernetes patches come weekly

- **Some patches requires node restart**
  - A bit dependent on underlying OS
  - Example: VMware - Photon, Microsoft – Mariner
- **Kured (Kubernetes Reboot Daemon)**
  - Look after /var/run/reboot-required and reboot if required
- **Node image upgrade**

K8s version	Upstream release	AKS preview	AKS GA	End of life
1.24	Apr-22-22	May 2022	Jul 2022	Jul 2023
1.25	Aug 2022	Oct 2022	Dec 2022	Dec 2023
1.26	Dec 2022	Feb 2023	Apr 2023	Mar 2024
1.27	Apr 2023	Jun 2023	Jul 2023	Jul 2024

Get warning about unsupported API's

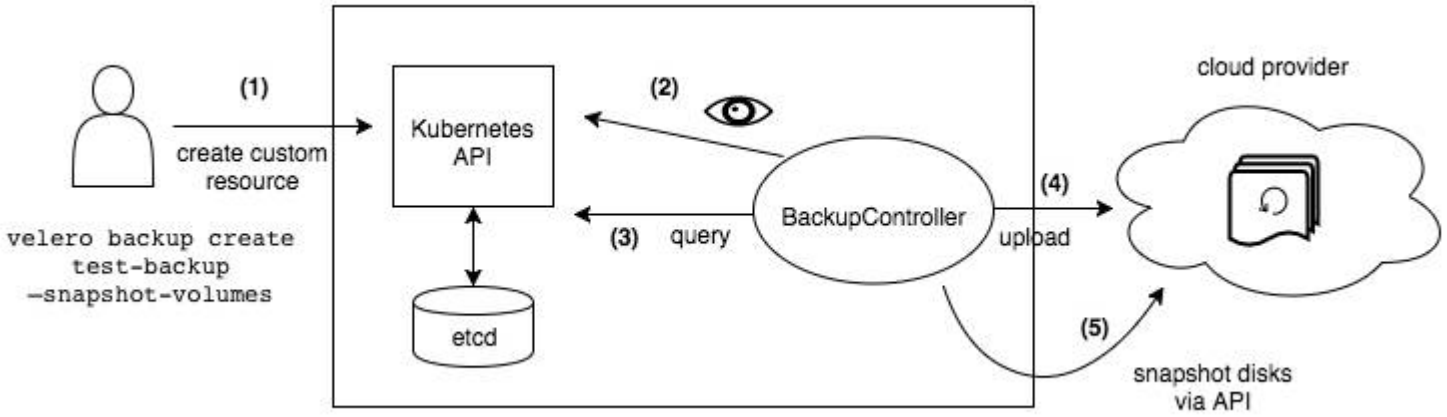
FairwindsOps/pluto

©2022 Microsoft Security User Group Norway All Rights Reserved

Backup and data protection

For services that require persistent storage

- Provisions using built-in CSI (storage interface)
  - Cloud platforms, Dell, HP, NetApp, IBM etc
- For data storage that requires read/write by multiple pods.
- Backup is something that needs to be deployed seperately
  - Use of tools like **Velero**, **Kasten** or **Portvorx Backup**



Kubestr can be used to benchmark CSI drivers

©2022 Microsoft Security User Group Norway All Rights Reserved

Pod Security Admission (PSA)

Better default isolation on containers

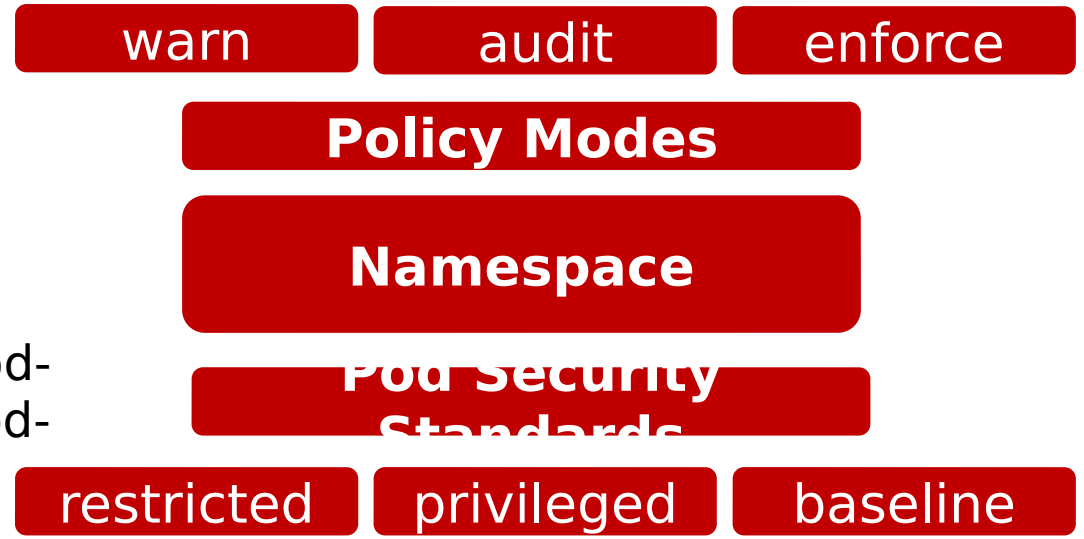
Can define different standards

Operate on a namespace level

Three built-in levels

Example: Privileged gives no limits

Can be defined on namespace level



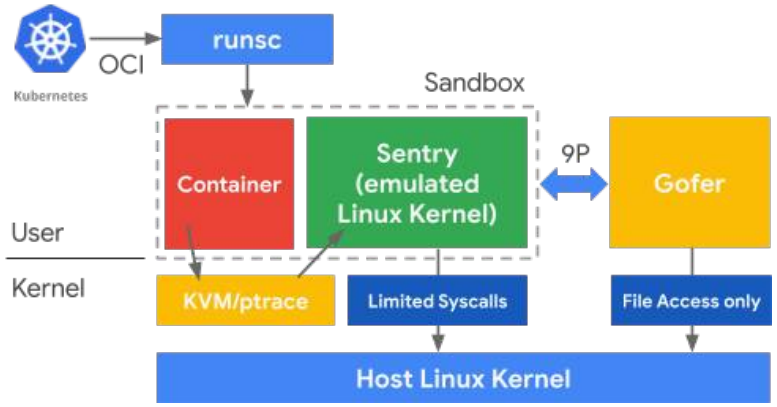
kubectl label --overwrite ns test-privileged pod-security.kubernetes.io/**enforce=privileged** pod-security.kubernetes.io/**warn=privileged**

kubectl label --overwrite ns test-restricted pod-security.kubernetes.io/**enforce=restricted** pod-security.kubernetes.io/**warn=restricted**

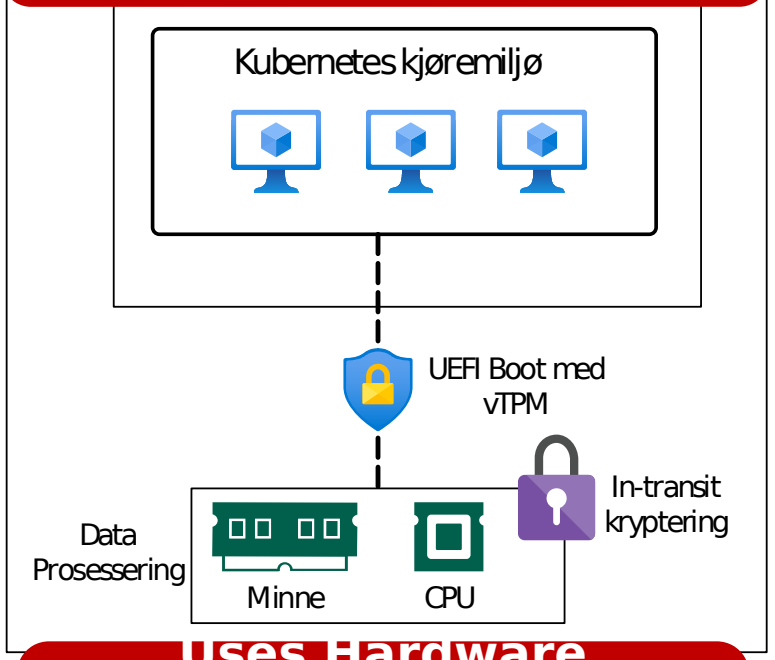
©2022 Microsoft Security User Group Norway All Rights Reserved

Encryption and Container Isolation

gVisor - emulates OS-Kernel calls to reduce the risk of container escape

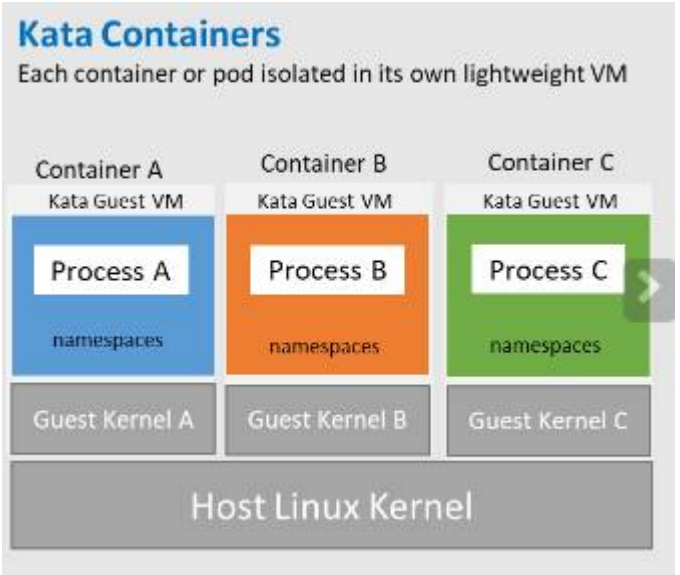


Confidental Computing on Public Cloud



Uses Hardware technology from AMD to encrypt everything in runtime

Kata Containers



Microsoft Security User Group Norway

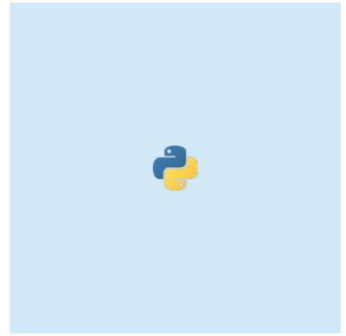
C2 - Restricted

©2022 Microsoft Security User Group Norway All Rights Reserved

github.com/msugn
@MsSecUGNorway
#MSUGN

Container Registry

- **Many are using base image with heavy footprin**
  - Small changes required such as just changing to slim
- **Private vs Public Image repository**
- **Same principles apply in regard to access contr**
- **Only allow «approved» images**
- **Image scanning mechanisms to detect vulnerab**
  - Quay / Clair
  - Falco
  - Trivy
  - Cloud providers



python

882 MB
431 dependencies
268 vulnerabilities
66 high severity

python: 3-slim-buster

113 MB
94 dependencies
75 vulnerabilities
1 high severity

Note: none of the high severity vulnerabilities currently have fixes available, nor do they have an exploit in the wild.

Microsoft Security User Group Norway

C2 - Restricted

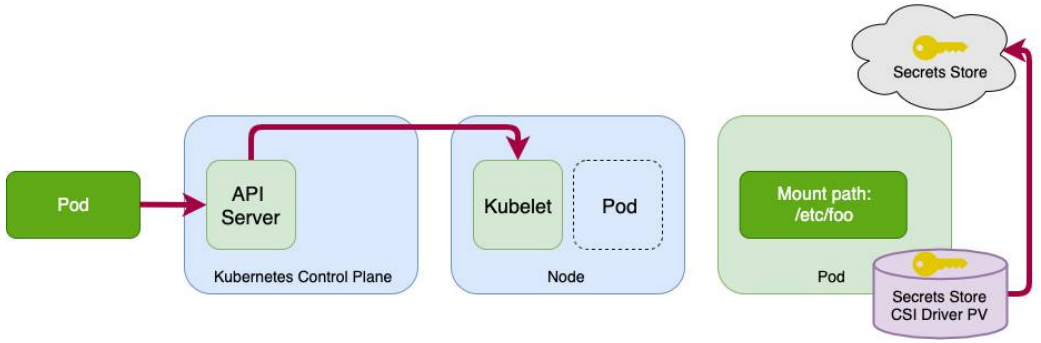
©2022 Microsoft Security User Group Norway All Rights Reserved

github.com/msugn
@MsSecUGNorway
#MSUGN

Secret Management

Caution:
Kubernetes Secrets are, by default, stored unencrypted in the API server's underlying data store (etcd). Anyone with API access can retrieve or modify a Secret, and so can anyone with access to etcd.
Additionally, anyone who is authorized to create a Pod in a namespace can use that access to read any Secret in that namespace; this includes indirect access such as the ability to create a Deployment.

- **Etcd has no built-in versioning or backup**
- **Data is not encrypted at rest by default**
- External Kubernetes Secret Operator or...
- Secret CSI driver



Features \ Providers	Azure	GCP	AWS	Vault
Sync as Kubernetes secret	Yes	Yes	Yes	Yes
Rotation	Yes	Yes	Yes	Yes
Windows	Yes	No	No	No
Helm Chart	Yes	No	No	Yes

Supported for Secret Store CSI

©2022 Microsoft Security User Group Norway All Rights Reserved

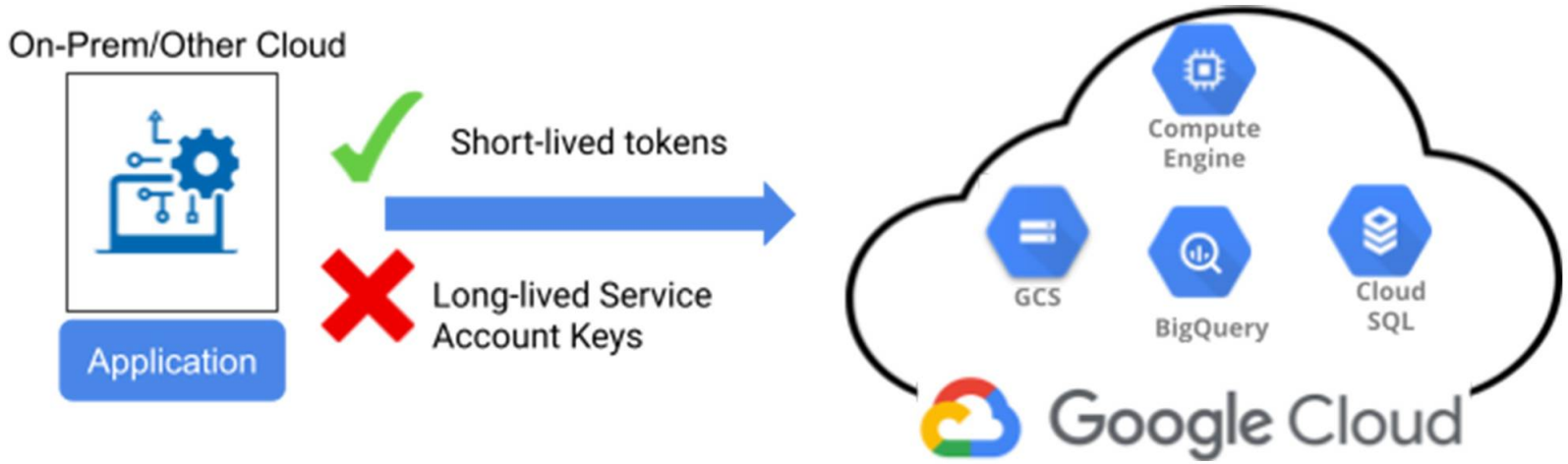
Workload Identity

Safe authentication between **container** to **PaaS services**

Supported by Google and Microsoft

Federate authentication trough OpenID Connect

Avoid use of keys at all! (at least only shortlived)



©2022 Microsoft Security User Group Norway All Rights Reserved

Kubernetes Nettverk - some acronyms

CNI = Network integration between Kubernetes and the underlying network

CRD = Custom Resource Definition (Utvidelse med ressurser I Kubernetes APIet)

Network Policies = Lag ¾ Firewall mechanisms – Controlled via CNI

Services = Exposing of a service in a pod

Ingress / Gateway API = Entry to the different services (trough layer 7)

IP Tables = packet filter in the OS kernel and controls much of the network logic in k8s

eBFP = Mini applications running as a sandbox package in the OS kernel

C2 - Restricted
©2022 Microsoft Security User Group Norway All Rights Reserved

Network Policies

- **Traffic control on layer ¾**
  - IP, Port, Protocol, Pod label
  - By default everything in Kubernetes is open
- **Require a CNI that can control traffic**
  - Calico, WeaveNet, Azure CNI, GKE CNI, Cilium (eBFP)
  - Flannel (does not support Network Policies)
  - Traffic flow controlled via YAML configuration

Some free tools to visualize flow
https://orca.tufin.io/netpol/
https://artturik.github.io/network-policy-viewer/

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: frontend-to-sqldatabase
  namespace: default
spec:
  podSelector:
    matchLabels:
      app: sqldatabase
  policyTypes:
  - Ingress
  - Egress
  ingress:
  - from:
    - ipBlock:
        cidr: 172.17.0.0/1
    - namespaceSelector:
        matchLabels:
          project: myproject
    - podSelector:
        matchLabels:
          role: frontend
  egress:
  - to:
    - ipBlock:
        cidr: 10.0.0.0/24
    ports:
    - protocol: TCP
      port: 5978
```

Target

Source IP

Source

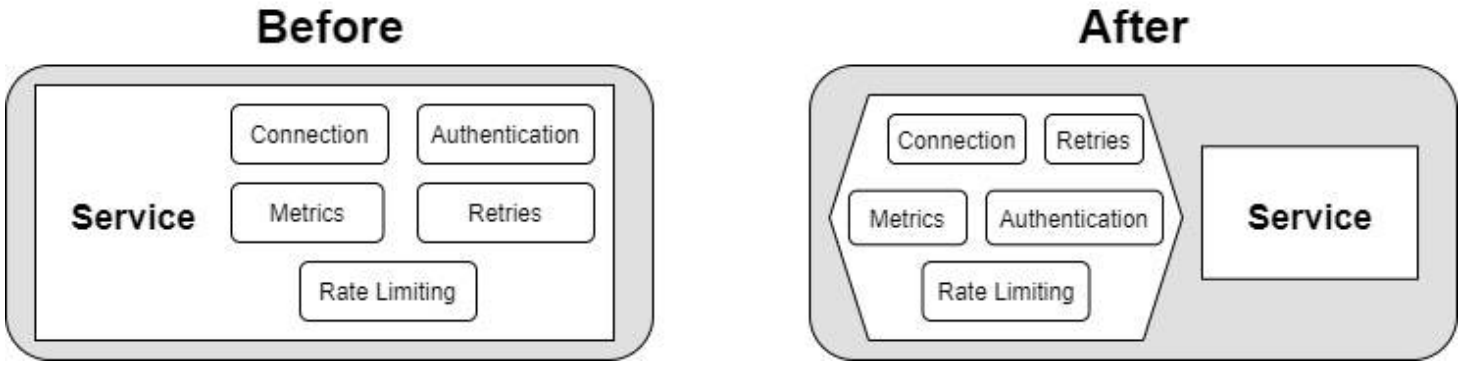
Target IP og Port

Microsoft Security User Group Norway
C2 Restricted
©2022 Microsoft Security User Group Norway All Rights Reserved

Service Mesh

Allows us to provide the following features in the platform

Visibilty (L7)
Security (L7)
Traffic shaping



Moving this functionality out of the application layer and into the platform

©2022 Microsoft Security User Group Norway All Rights Reserved

Service Mesh - Architecture

Different features and architecture depending on vendor

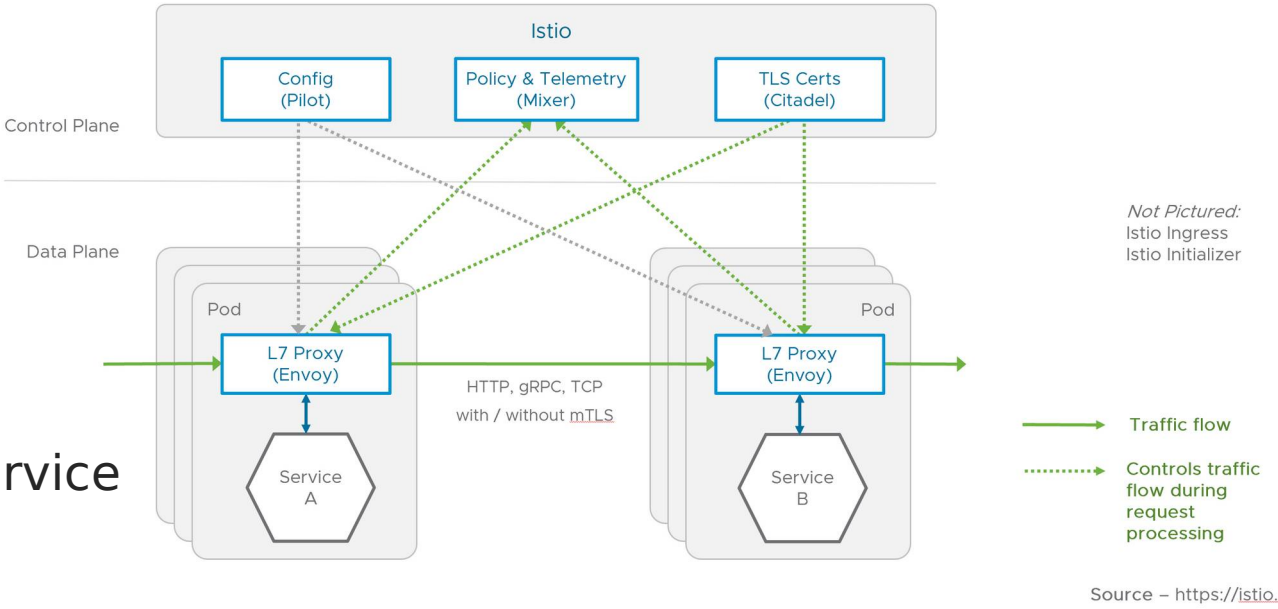
Sidecar proxy or use of eBFP

- Cilium use eBFP
- Istio use iptables
- Provides for instance mTLS on service-to-service

Provides visibility into the network tier

Layer 7 network policies

Service Mesh architecture will soon be replaced with a new architecture



Architecture based upon Isitio which uses Envoy as a sidecar proxy

©2022 Microsoft Security User Group Norway All Rights Reserved

Some Service Mesh alternatives

Features	Istio	Linkerd	Hashicorp Consul	Traefik Mesh	Kuma (fra Kong)	Open Service Mesh	VMware Tanzu
Proxy component	Envoy	Linkerd2-proxy	Envoy	Egen	Envoy	Envoy	Envoy
Sidecar Proxy	Yes	Yes	Yes	No	Yes	Yes	Yes
Container-VM	Yes	No	Yes	No	Yes	No	No
MultiCluster	Yes	Yes	Yes	No	Yes		Yes
BYO Ingress	Gateway	Yes	Yes	Wel..	Yes	Yes	Yes
Dashboard	Kiali	Yes	Yes	Traefik Hub		Azure Monitor	Tanzu Mission Control
mTLS	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Traffic Kontroll	Yes	Yes	Yes	Yes	Yes	Yes	Yes
HTTP/3	Yes	No	Yes	Yes	Yes	Yes	Yes

C2 - Restricted
©2022 Microsoft Security User Group Norway All Rights Reserved

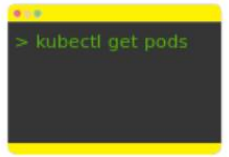
Security Monitoring of Kubernetes

Kubernetes API monitoring

DNS Logs from CoreDNS

Host logs

CNI logs



Kubectl apply -f

Kubernetes Audit Policy

Audit Level

- None
- Metadata
- Request
- RequestResponse

```
apiVersion: audit.k8s.io/v1
kind: Policy
omitStages:
- "RequestReceived"
rules:
- level: RequestResponse
resources:
- group: ""
resources: ["pods"]
- level: Metadata
resources:
- group: ""
resources: ["pods/log",
"pods/status"]
```

Log service

- Splunk
- Sentinel
- ELK
- Loki

[Customize Azure Kubernetes Service Diagnostics for Azure Log Analytics - msandbu.org]

Microsoft Security User Group Norway

C2 - Restricted

©2022 Microsoft Security User Group Norway All Rights Reserved

github.com/msugn
@MsSecUGNorway
#MSUGN

Enterprise products

- ✓ Secure Code development
- ✓ Securing dependencies
- ✓ Container Image Scanning
- ✓ Secure IaC

- ✓ Secure Code Development
- ✓ Secure IaC

- ✓ Cloud and Kubernetes Security Posture
- ✓ Secure Code Development
- ✓ Securing Pipelines
- ✓ Secure IaC
- ✓ Vulnerability Management

- ✓ Cloud and Kubernetes Security Posture
- ✓ Secure Code Development
- ✓ Securing Pipelines
- ✓ Secure IaC
- ✓ Vulnerability Management

©2022 Microsoft Security User Group Norway All Rights Reserved

So where to start?

Basic Mechanisms

- ✓ Private Cluster
- ✓ Identity based access
- ✓ Security scanning for vulnerabilities and dependencies
- ✓ Simple network Policies
- ✓ Control of versioning

Next level of maturity

- ✓ Workload Identity
- ✓ Security Monitoring
- ✓ External Secret Management
- ✓ Proper Network Policies based upon Zero-trust principles
- ✓ GitOps
- ✓ Identity control using SCIM

Per use-case

- ✓ Service Mesh
- ✓ Backup
- ✓ Kubebench (CIS, NIST validering)
- ✓ Confidential Computing or Kata VM
- ✓ Use of enterprise commersial producuts
- ✓ Falco/Tetragon

Build understanding

Train the developers

Start with simple achiveable goals

C2 - Restricted
©2022 Microsoft Security User Group Norway All Rights Reserved

Microsoft Security

USER GROUP NORWAY

C2 - Restricted