

Microsoft Defender for Cloud

Defender for Containers

Demo in a multi-cloud environment lab

Stefano Pescosolido

Microsoft Technical Specialist – Cybersecurity

stefano.pescosolido@microsoft.com

Microsoft Defender for Containers

Protect multi-cloud and hybrid container deployments



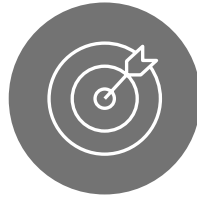
Hardening

Continuously assess and improve the security posture of your containerized environments and workloads



Vulnerability management

Reduce your attack surface by continuously scanning workloads to identify and manage container vulnerabilities



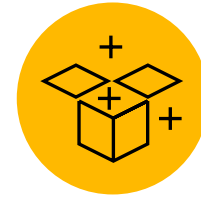
Advanced threat detection

Identify runtime threats with prioritized, container-specific alerts – using powerful insights from Microsoft Threat Intelligence



Multi-cloud support

Single container security solution for Kubernetes clusters, across Azure, AWS, GCP and on-premise

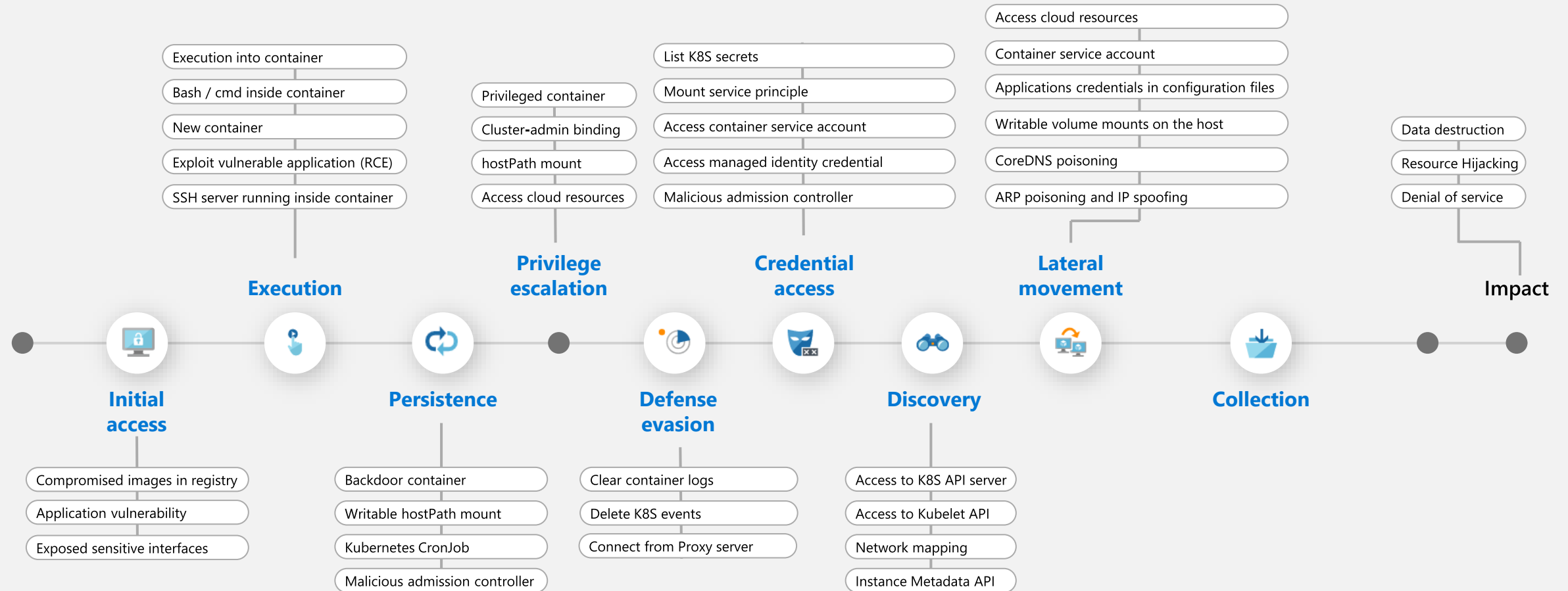


Deployment and monitoring

Frictionless deployment provisioning at scale with easy onboarding and support for standard Kubernetes monitoring tools



Threat detections aligned to the Kubernetes Attack Matrix



Solution components

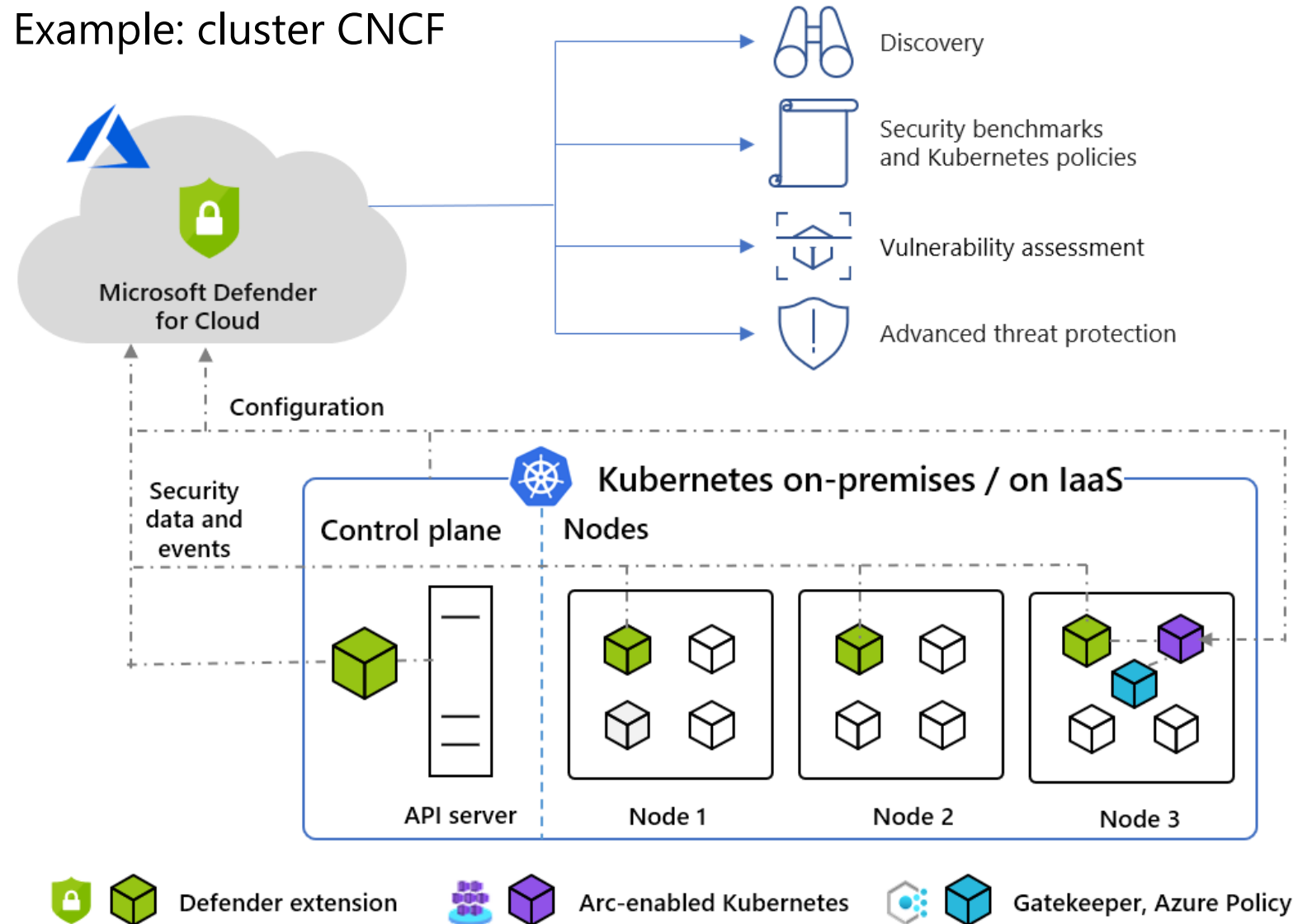
Workloads for:

- The connection to **Azure Arc** (enabled K8s)
- **Defender Extension** (DaemonSet)
- **Azure Policy Extension** (w/ Gatekeeper)

In EKS and GKE there is a different mechanism for K8s audit collection.

In AKS there are no Arc component, the Azure Policy is connected through an add-in and the audit log collection is native,

Example: cluster CNCF



aws Services
Google Cloud containers
adm73 @ 7228-7345-1517

Amazon Elastic Kubernetes Service

[Clusters](#) New

▼ Related services

Amazon ECR
Container storage for EKS

Documentation [↗](#)

Submit feedback

Compute Engine

Virtual machines

- VM instances
- Instance templates
- Sole-tenant nodes
- Machine images
- TPUs
- Committed use discounts
- Migrate to Virtual Machin...

Storage

- Disks
- Snapshots
- Images

Instance groups

- Marketplace
- Release Notes

VM instances

304251bu-x1sc

<input type="checkbox"/>	<input checked="" type="checkbox"/>	ubuntu	us-central1-c	SSH	⋮
<input type="checkbox"/>	<input checked="" type="checkbox"/>	vm-k8sfnd-cp	us-central1-c	SSH	⋮
<input type="checkbox"/>	<input checked="" type="checkbox"/>	vm-k8sfnd-wkr-1	us-central1-c	SSH	⋮

Related actions ^ HIDE

Explore Actifio GO

Back up your VMs and set up disaster recovery

View billing report

View and manage your Compute Engine billing

Monitor VMs

View outlier VMs across metrics like CPU and network

Explore VM logs

View, search, analyze, and download VM instance logs

Set up firewall rules

Control traffic to and from a VM instance

Patch management

Schedule patch updates and view patch compliance on VM instances

Tags

< 1 >

Status ▾

✔ Ready

de group

Status ▾

✔ Active

Terms [Cookie preferences](#)

Home > Azure Arc

Azure Arc | Kubernetes clusters

Search (Ctrl+/)

- Overview
- All Azure Arc resources

Management

- Custom locations
- Data controllers
- Resource bridges (preview)
- Service principals
- Private link scopes

Infrastructure

- Azure Arc virtual machines (preview)
- Azure Stack HCI
- Kubernetes clusters**
- Servers
- SQL Servers
- VMware vCenters (preview)

[+ Add a Kubernetes cluster with Azure Arc](#)
[Manage view](#)
[Refresh](#)
[Export to CSV](#)
[Open query](#)
[Assign tags](#)

Filter for any field...

Subscription equals **StefanPe MS Internal Lab**




Resource group equals **all**

Location equals **all**

[+ Add filter](#)

No grouping

List view

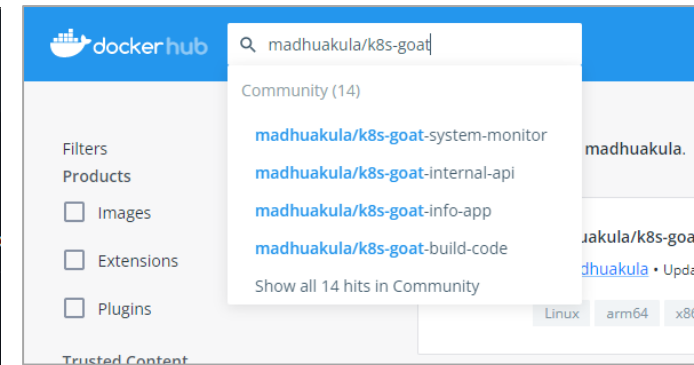
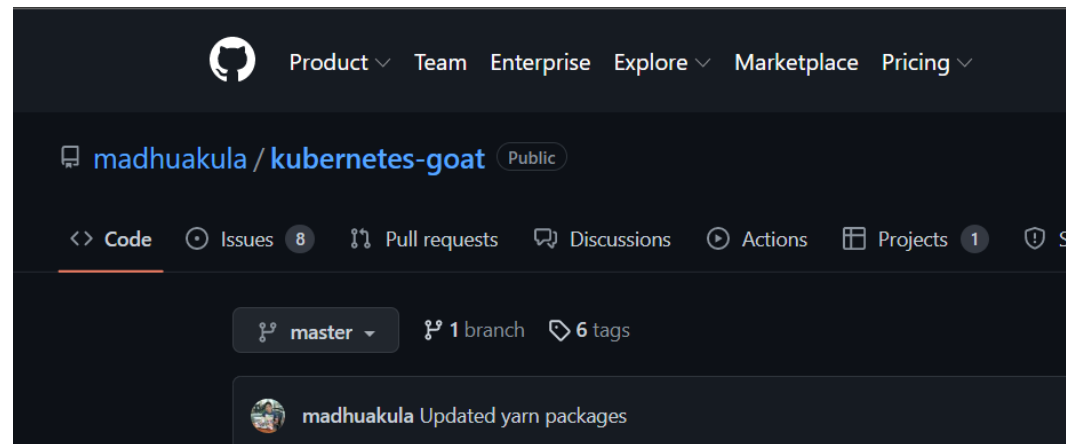
<input type="checkbox"/>	Name ↑↓	Type ↑↓	Resource group ↑↓	Kuberne... ↑↓	Location ↑↓	Subscription ↑↓
<input type="checkbox"/>	 eks-cluster-1	Kubernetes - Azure Arc	rgmulticloud	1.22.11-eks-1...	Central US	StefanPe MS Internal L... ⋮
<input type="checkbox"/>	 gke-std-cluster-pub-1-us-central1-c-8850...	Kubernetes - Azure Arc	rgMultiCloud	1.22.11-gke.4...	Central US	StefanPe MS Internal L... ⋮
<input type="checkbox"/>	 k8s-cncf-gcp-1	Kubernetes - Azure Arc	rgArcK8s	1.23.1	West Europe	StefanPe MS Internal L... ⋮

< Previous Page 1 of 1 Next > Showing 1 to 3 of 3 records.

[Give feedback](#)

Resources and experiences used in my lab

- [Kubernetes Goat | Kubernetes Goat \(madhuakula.com\)](https://madhuakula.com) – By [Madhu Akula](#)
- [A look at how Defender for Containers protects your clusters \(guillaumeben.xyz\)](https://guillaumeben.xyz) – By [Guillaume Benats](#)



- <https://madhuakula.com/kubernetes-goat/docs/>
- <https://github.com/madhuakula/kubernetes-goat>
- <https://hub.docker.com/search?q=madhuakula>
- <https://guillaumeben.xyz/defender-containers.html>



acrstefanpe1 | Repositories



Container registry

Directory: stefanpedev

Search (Ctrl+)



Refresh



Overview



Activity log



Access control (IAM)



Tags



Quick start



Events

Settings



Access keys



Encryption



Identity



Networking



Microsoft Defender for Cloud



Locks

Services



Repositories



Webhooks



Replications



Search to filter repositories ...

Repositories ↑↓

[k8s-goat-batch-check](#)

[k8s-goat-build-code](#)

[k8s-goat-cache-store](#)

[k8s-goat-health-check](#)

[k8s-goat-helm-tiller](#)

[k8s-goat-hidden-in-layers](#)

[k8s-goat-home](#)

[k8s-goat-hunger-check](#)

[k8s-goat-info-app](#)

[k8s-goat-metadata-db](#)

[k8s-goat-poor-registry](#)

[k8s-goat-system-monitor](#)

Demo



Thank you