CIS Amazon EKS Benchmark

Securing cluster node configurations

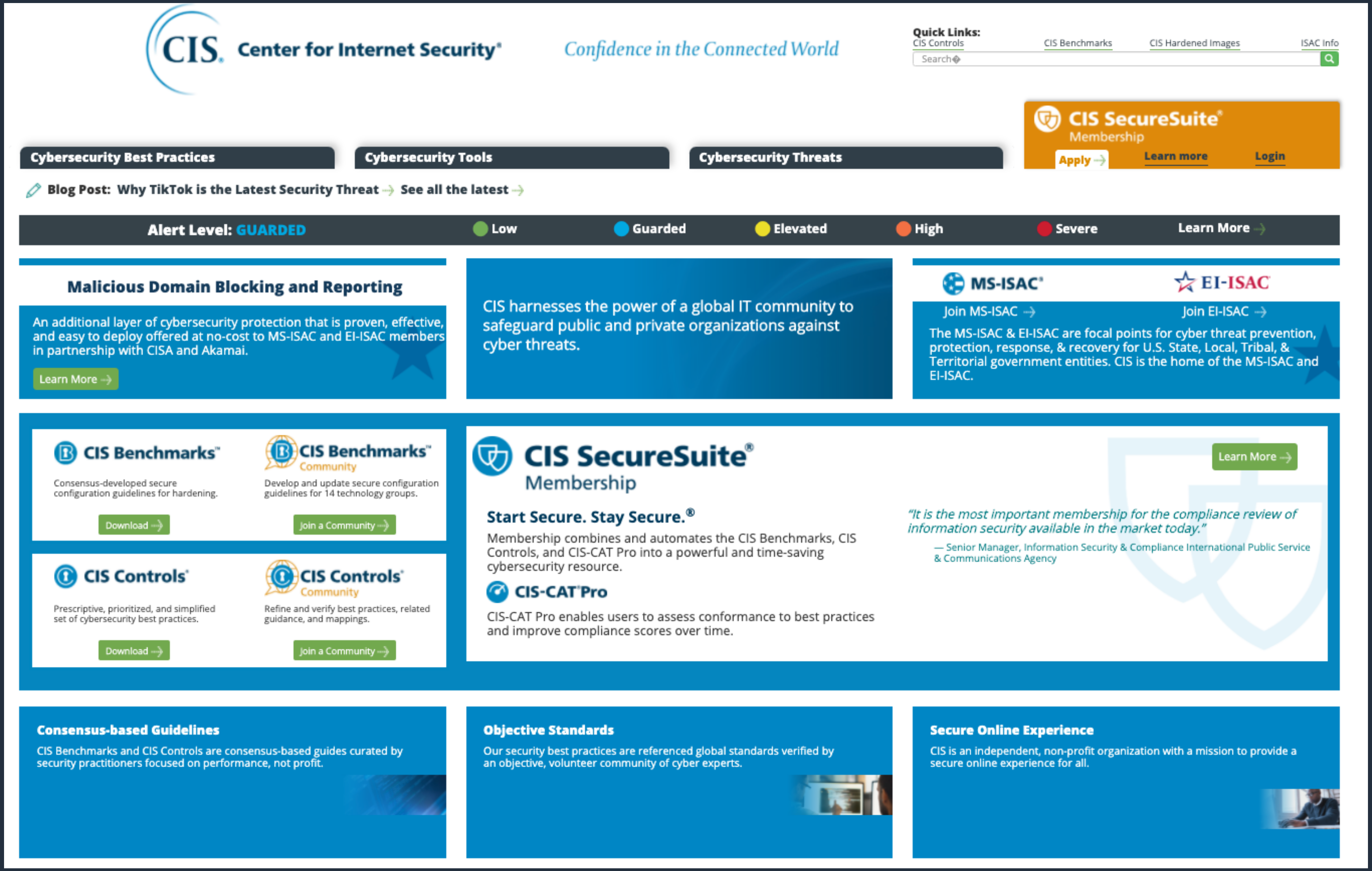
Paavan Mistry – Senior Developer Advocate, AWS
August 17th 2020

Table of contents

- CISecurity.org and the CIS Kubernetes Benchmark
- The Shared Responsibility Model for Amazon EKS
- CIS Amazon EKS Benchmark
- “Show me how to use this Benchmark” - Demo

CISecurity.org and the CIS Kubernetes Benchmark

CISecurity.org



CIS. Center for Internet Security®

Confidence in the Connected World

Quick Links: CIS Controls | CIS Benchmarks | CIS Hardened Images | ISAC Info

Search�

Blog Post: Why TikTok is the Latest Security Threat → **See all the latest →**

Alert Level: GUARDED ● Low ● Guarded ● Elevated ● High ● Severe **Learn More →**

Malicious Domain Blocking and Reporting

An additional layer of cybersecurity protection that is proven, effective, and easy to deploy offered at no-cost to MS-ISAC and EI-ISAC members in partnership with CISA and Akamai.

CIS harnesses the power of a global IT community to safeguard public and private organizations against cyber threats.

The MS-ISAC & EI-ISAC are focal points for cyber threat prevention, protection, response, & recovery for U.S. State, Local, Tribal, & Territorial government entities. CIS is the home of the MS-ISAC and EI-ISAC.

CIS Benchmarks™

Consensus-developed secure configuration guidelines for hardening.

CIS Benchmarks™ Community

Develop and update secure configuration guidelines for 14 technology groups.

CIS Controls®

Prescriptive, prioritized, and simplified set of cybersecurity best practices.

CIS Controls® Community

Refine and verify best practices, related guidance, and mappings.

CIS SecureSuite® Membership

Start Secure. Stay Secure.®

Membership combines and automates the CIS Benchmarks, CIS Controls, and CIS-CAT Pro into a powerful and time-saving cybersecurity resource.

CIS-CAT®Pro

CIS-CAT Pro enables users to assess conformance to best practices and improve compliance scores over time.

"It is the most important membership for the compliance review of information security available in the market today."

— Senior Manager, Information Security & Compliance International Public Service & Communications Agency

Consensus-based Guidelines

CIS Benchmarks and CIS Controls are consensus-based guides curated by security practitioners focused on performance, not profit.

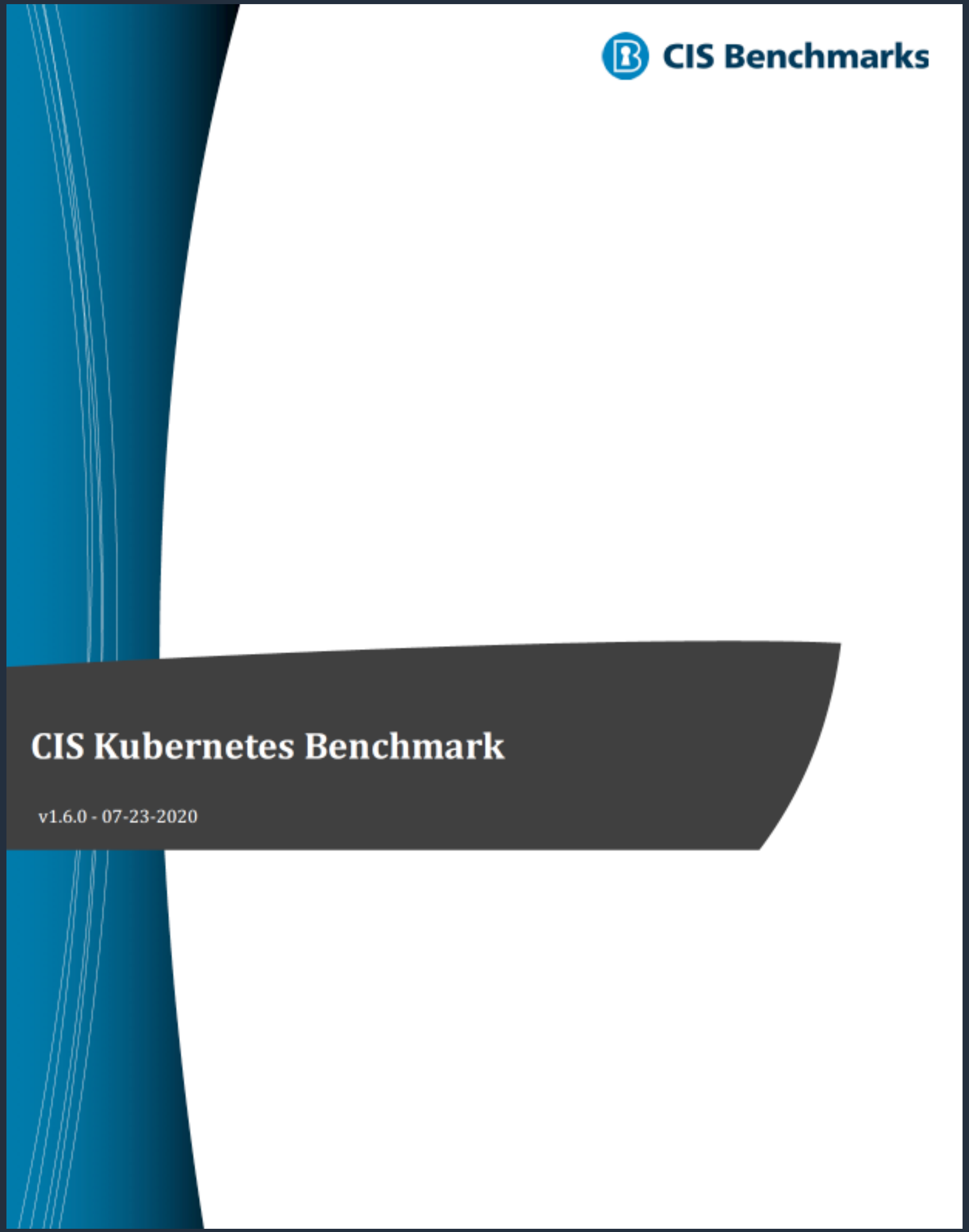
Objective Standards

Our security best practices are referenced global standards verified by an objective, volunteer community of cyber experts.

Secure Online Experience

CIS is an independent, non-profit organization with a mission to provide a secure online experience for all.

CIS Kubernetes Benchmark



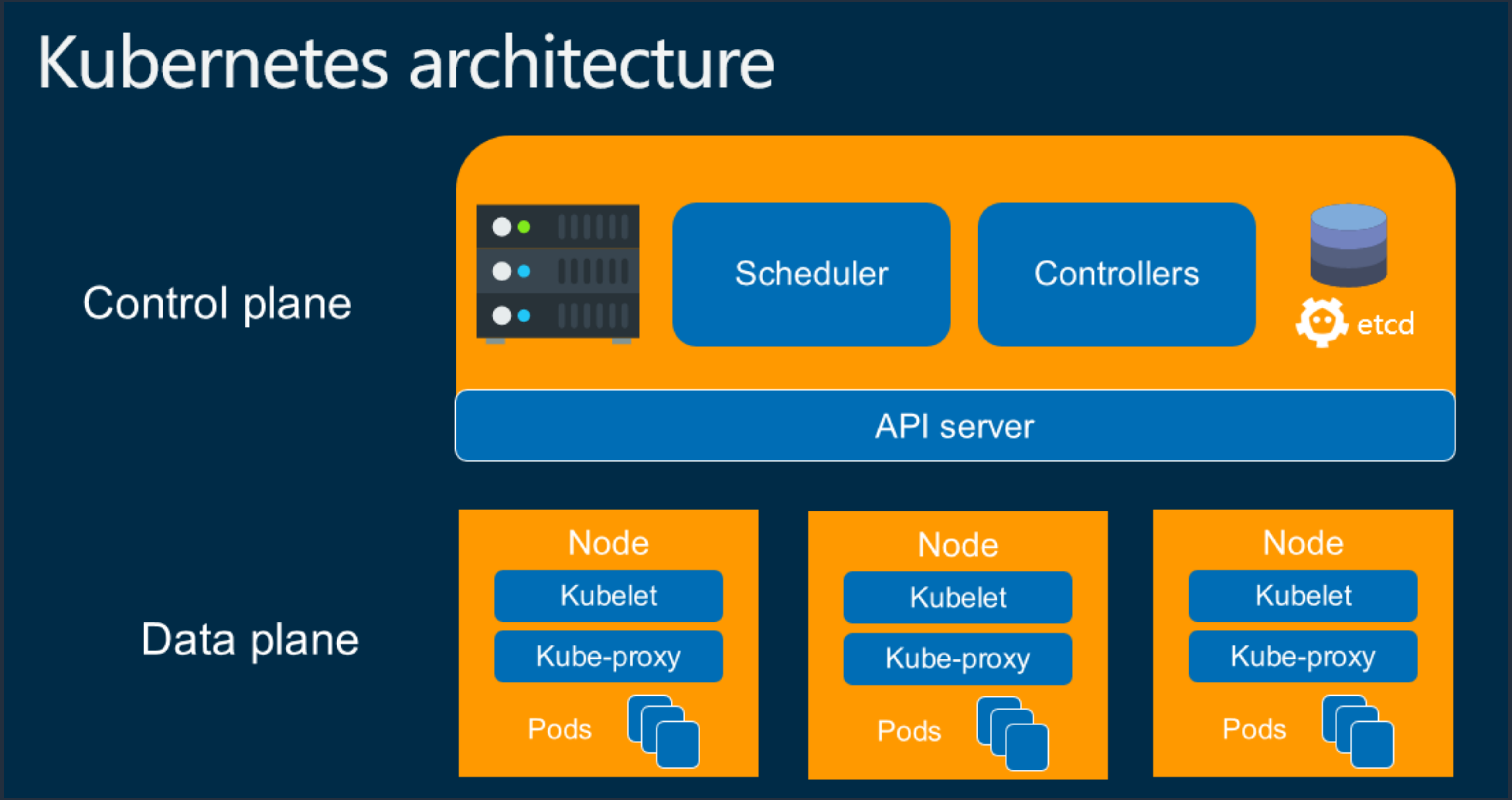
CIS Benchmarks

CIS Kubernetes Benchmark

v1.6.0 - 07-23-2020

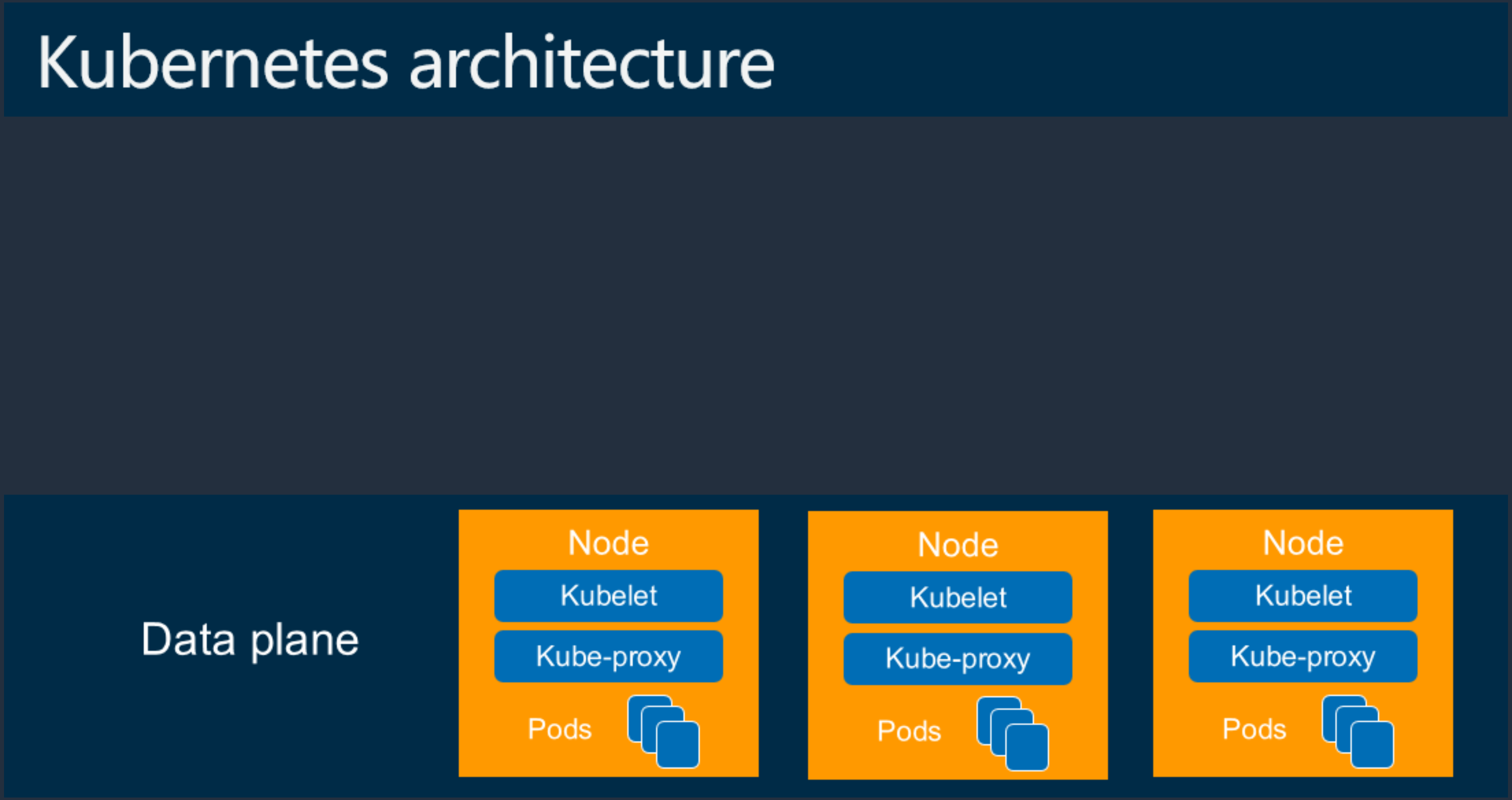
- Initially published in May 2017
- Community-driven and consensus-based security good practice guidance
- Currently publication (v1.6.0) supports Kubernetes v1.16 – v1.18
- Industry-accepted system hardening procedures
- Reviewed by Kubernetes community contributors and subject matter experts

CIS Kubernetes Benchmark – Guidance scope



Shared Responsibility Model – Amazon EKS

Managed Kubernetes – Amazon EKS



Kubernetes architecture

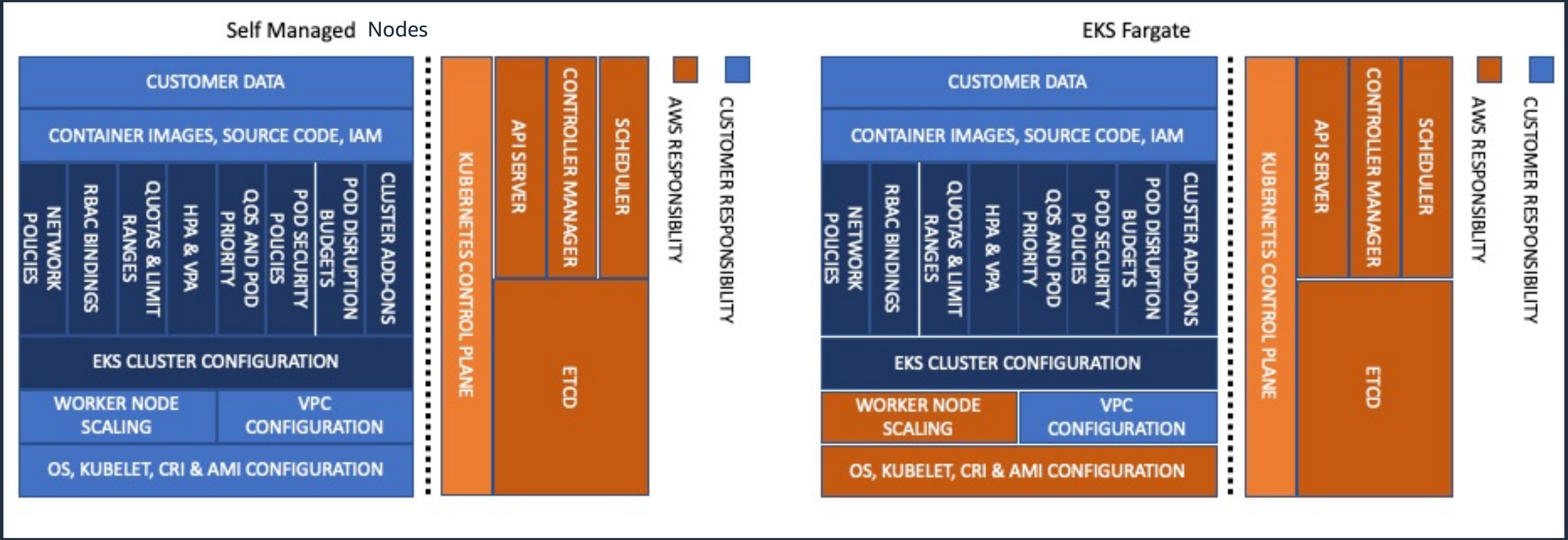
Data plane

Node
Kubelet
Kube-proxy
Pods

Node
Kubelet
Kube-proxy
Pods

Node
Kubelet
Kube-proxy
Pods

Amazon EKS – Shared Responsibility Model



Self Managed Nodes

CUSTOMER DATA

CONTAINER IMAGES, SOURCE CODE, IAM

NETWORK POLICIES

RBAC BINDINGS

QUOTAS & LIMIT RANGES

HPA & VPA

QOS AND POD PRIORITY

POD SECURITY POLICIES

POD DISRUPTION BUDGETS

CLUSTER ADD-ONS

EKS CLUSTER CONFIGURATION

WORKER NODE SCALING

VPC CONFIGURATION

OS, KUBELET, CRI & AMI CONFIGURATION

KUBERNETES CONTROL PLANE

API SERVER

CONTROLLER MANAGER

SCHEDULER

ETCD

🟧 AWS RESPONSIBLITY

🟦 CUSTOMER RESPONSIBILITY

EKS Fargate

CUSTOMER DATA

CONTAINER IMAGES, SOURCE CODE, IAM

NETWORK POLICIES

RBAC BINDINGS

QUOTAS & LIMIT RANGES

HPA & VPA

QOS AND POD PRIORITY

POD SECURITY POLICIES

POD DISRUPTION BUDGETS

CLUSTER ADD-ONS

EKS CLUSTER CONFIGURATION

WORKER NODE SCALING

VPC CONFIGURATION

OS, KUBELET, CRI & AMI CONFIGURATION

KUBERNETES CONTROL PLANE

API SERVER

CONTROLLER MANAGER

SCHEDULER

ETCD

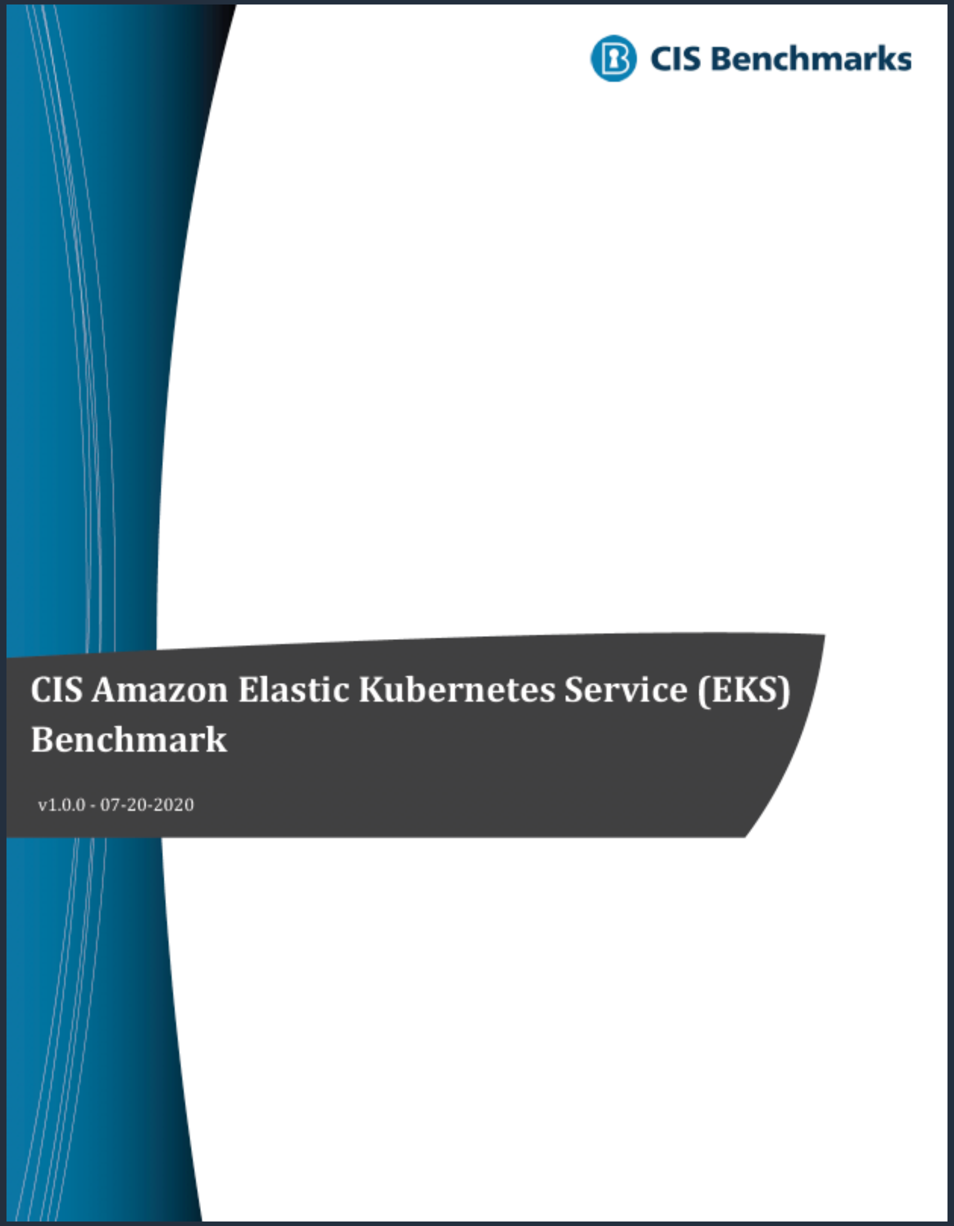
🟧 AWS RESPONSIBLITY

🟦 CUSTOMER RESPONSIBILITY

Source: https://aws.github.io/aws-eks-best-practices/

CIS Amazon EKS Benchmark

CIS Amazon EKS Benchmark



CIS Benchmarks

CIS Amazon Elastic Kubernetes Service (EKS) Benchmark

v1.0.0 - 07-20-2020

- Helps you accurately assess the security configuration of nodes running as part of your Amazon EKS clusters
- Applicable to EC2 nodes (both managed and self-managed)
- Consists of four sections:
  - Control plan logging configuration
  - Node security configurations
  - Policies
  - Managed services

Assessments using `kube-bench`

- Provide a mechanism to assess the node security configuration using `kube-bench` from the raw benchmark

- `kube-bench` is an open source tool created and maintained by Aqua Security, an AWS Advanced Technology Partner

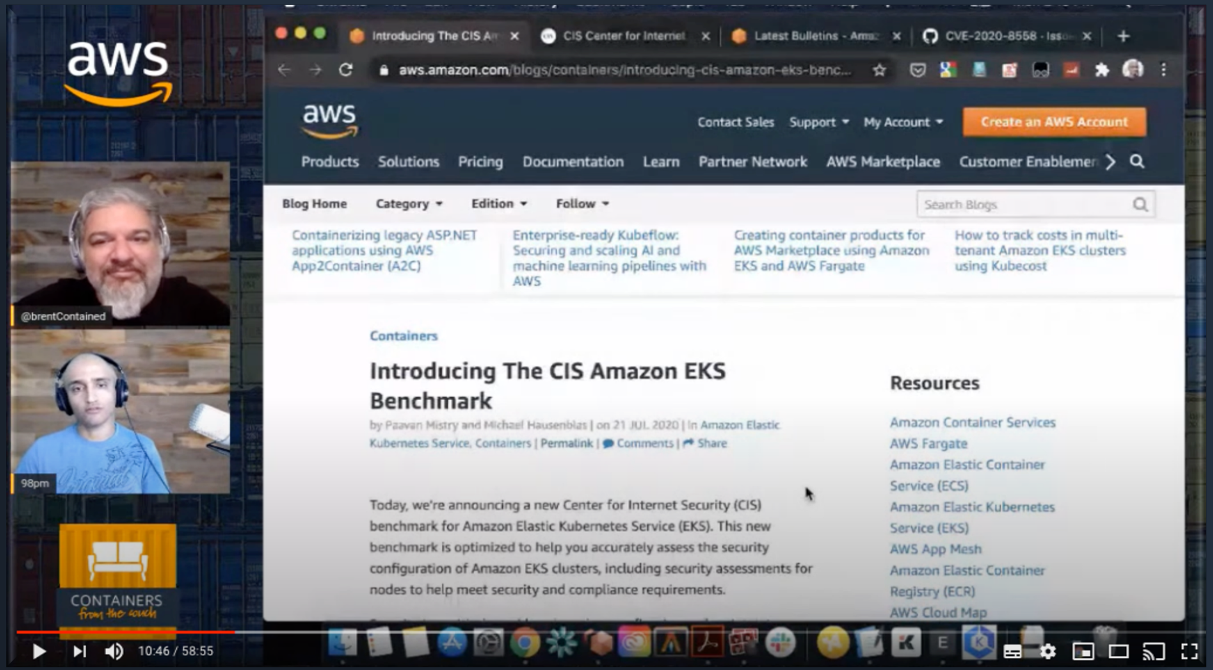
- Introduces an opportunity to automate node security assessments against the CIS Amazon EKS Benchmark for your Amazon EKS clusters

Demo – Show me how to use this Benchmark!

Resources and call to action

- Blog:
    - https://aws.amazon.com/blogs/containers/introducing-cis-amazon-eks-benchmark/

- 1 hour deep dive on #ContainersFromTheCouch show:
    - https://www.youtube.com/watch?v=m-3tMXmWWQw



Containerizing legacy ASP.NET applications using AWS App2Container (A2C)

Enterprise-ready Kubeflow: Securing and scaling AI and machine learning pipelines with AWS

Creating container products for AWS Marketplace using Amazon EKS and AWS Fargate

How to track costs in multi-tenant Amazon EKS clusters using Kubecost

Containers

Introducing The CIS Amazon EKS Benchmark

by Paavan Mistry and Michael Hausenblas | on 21 JUL 2020 | in Amazon Elastic Kubernetes Service, Containers | Permalink | Comments | Share

Today, we're announcing a new Center for Internet Security (CIS) benchmark for Amazon Elastic Kubernetes Service (EKS). This new benchmark is optimized to help you accurately assess the security configuration of Amazon EKS clusters, including security assessments for nodes to help meet security and compliance requirements.

Resources

- Amazon Container Services
- AWS Fargate
- Amazon Elastic Container Service (ECS)
- Amazon Elastic Kubernetes Service (EKS)
- AWS App Mesh
- Amazon Elastic Container Registry (ECR)
- AWS Cloud Map

- CIS Amazon EKS Benchmark: https://cisecurity.org/cis-benchmarks

Q&A

Ask on chat or visit our virtual booth during KubeCon EU 2020!

Thank you

Mail: paavan@amazon.com
Twitter: @98pm