BUTTERFLY EFFECT

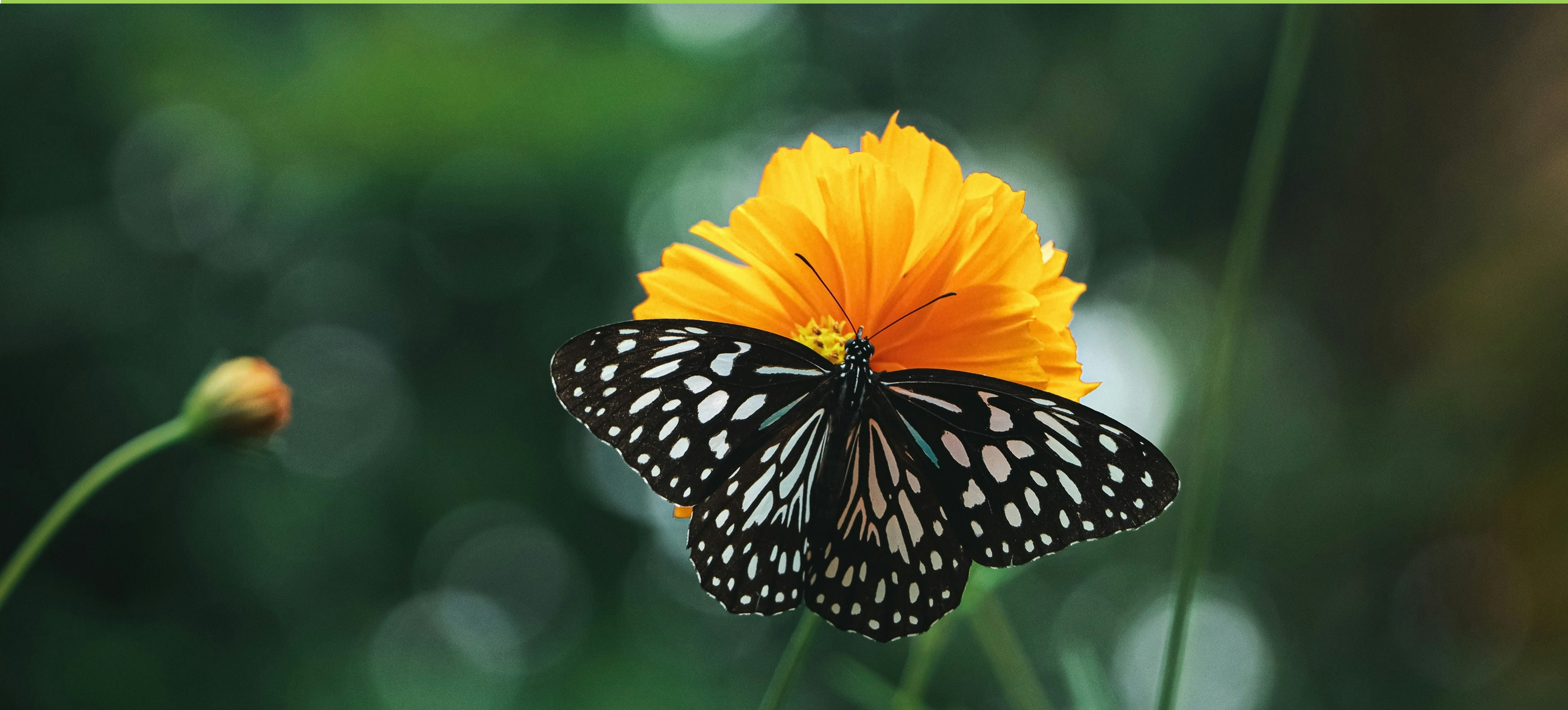
WHAT KUBERNETES SIG SECURITY HAS IN FLIGHT

Carol Valencia
Savitha Raghunathan
Ian Coldwater
Tabitha Sable

KubeCon | CloudNativeCon
North America 2025

KUBERNETES SIG SECURITY

KubeCon | CloudNativeCon
North America 2025



EVOLUTION

KubeCon | CloudNativeCon
North America 2025

SPREADING OUR WINGS

KubeCon | CloudNativeCon
North America 2025

THIRD-PARTY AUDIT

KubeCon | CloudNativeCon
North America 2025

SIG SECURITY DOCS

KubeCon | CloudNativeCon
North America 2025

OWASP KUBERNETES TOP TEN

KubeCon | CloudNativeCon
North America 2025

SIG Security is revamping the OWASP Kubernetes Top Ten!

We are planning to publish it by end of this year.

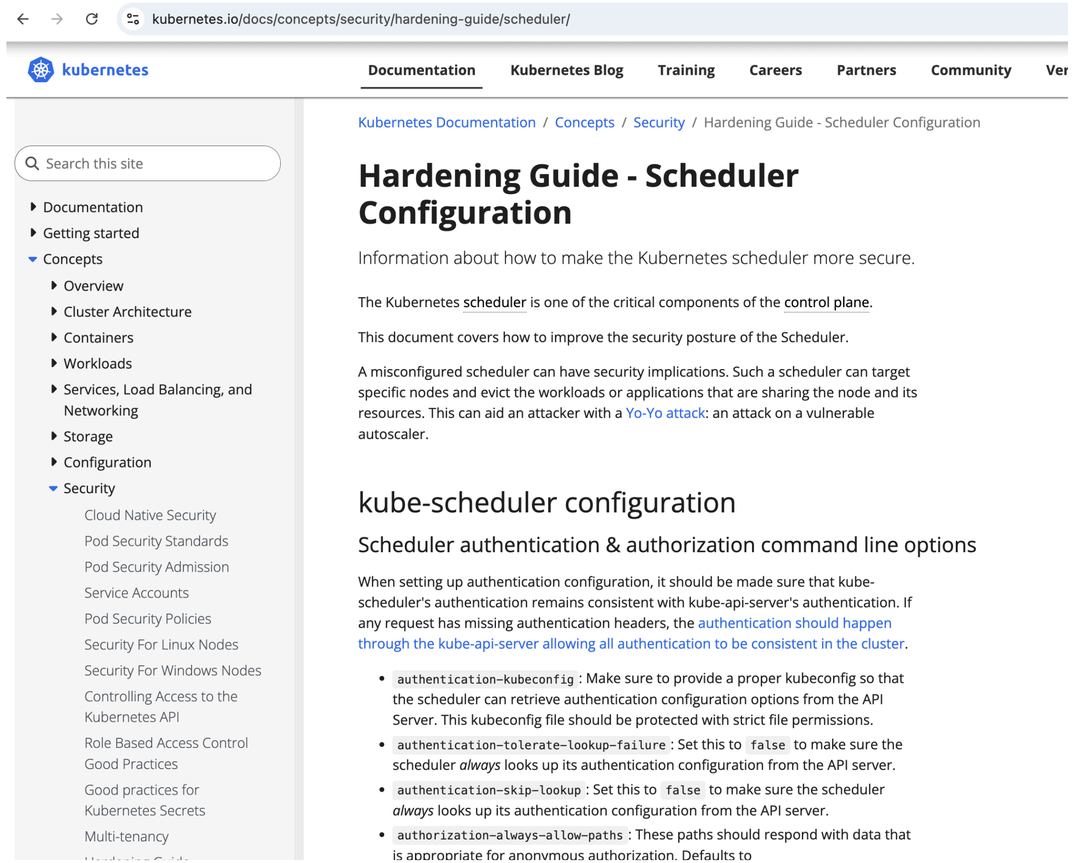
If you are interested in helping us curate the list and/or
contribute to a section, please reach out to us via slack channel.

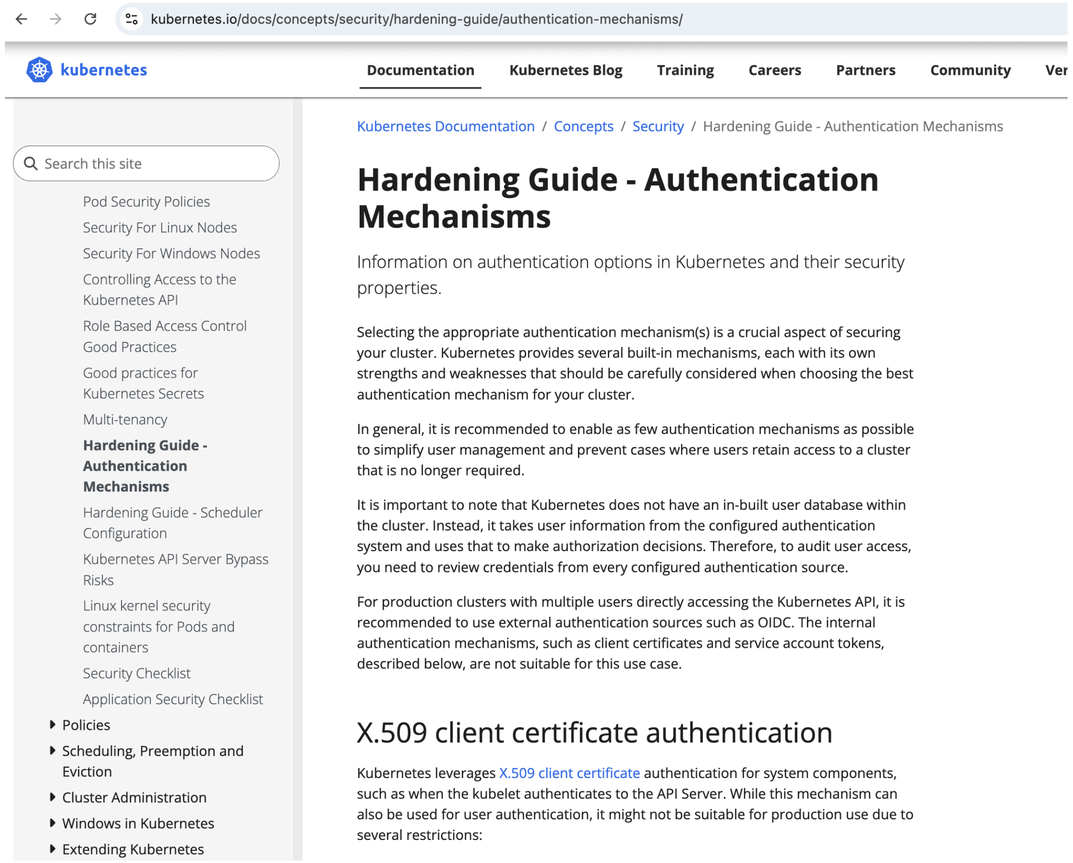
We want to hear from you!
Take the survey here:

HARDENING GUIDE

KubeCon | CloudNativeCon North America 2025

Hardening guide - https://github.com/kubernetes/sig-security/issues/30





HARDENING GUIDE

KubeCon | CloudNativeCon
North America 2025

Examples:

- Threat Model
- API Server Configuration
- Controller Manager Configuration
- File Permissions
- Worker Node Configuration
- PKI Management
- Authorization
- Workload Security Configuration
- Network Policy Configuration
- Add-On Configuration
- etcd

BRING YOUR IDEAS

KubeCon | CloudNativeCon
North America 2025

If you have an idea to improve the security content of the Kubernetes website, please feel free to start a thread in the Slack channel and/or create an issue in the k/website repo.

TOOLING

KubeCon | CloudNativeCon
North America 2025

TOOLING

SELF-ASSESSMENTS

KubeCon | CloudNativeCon
North America 2025

SELF-ASSESSMENTS 101

Define the scope

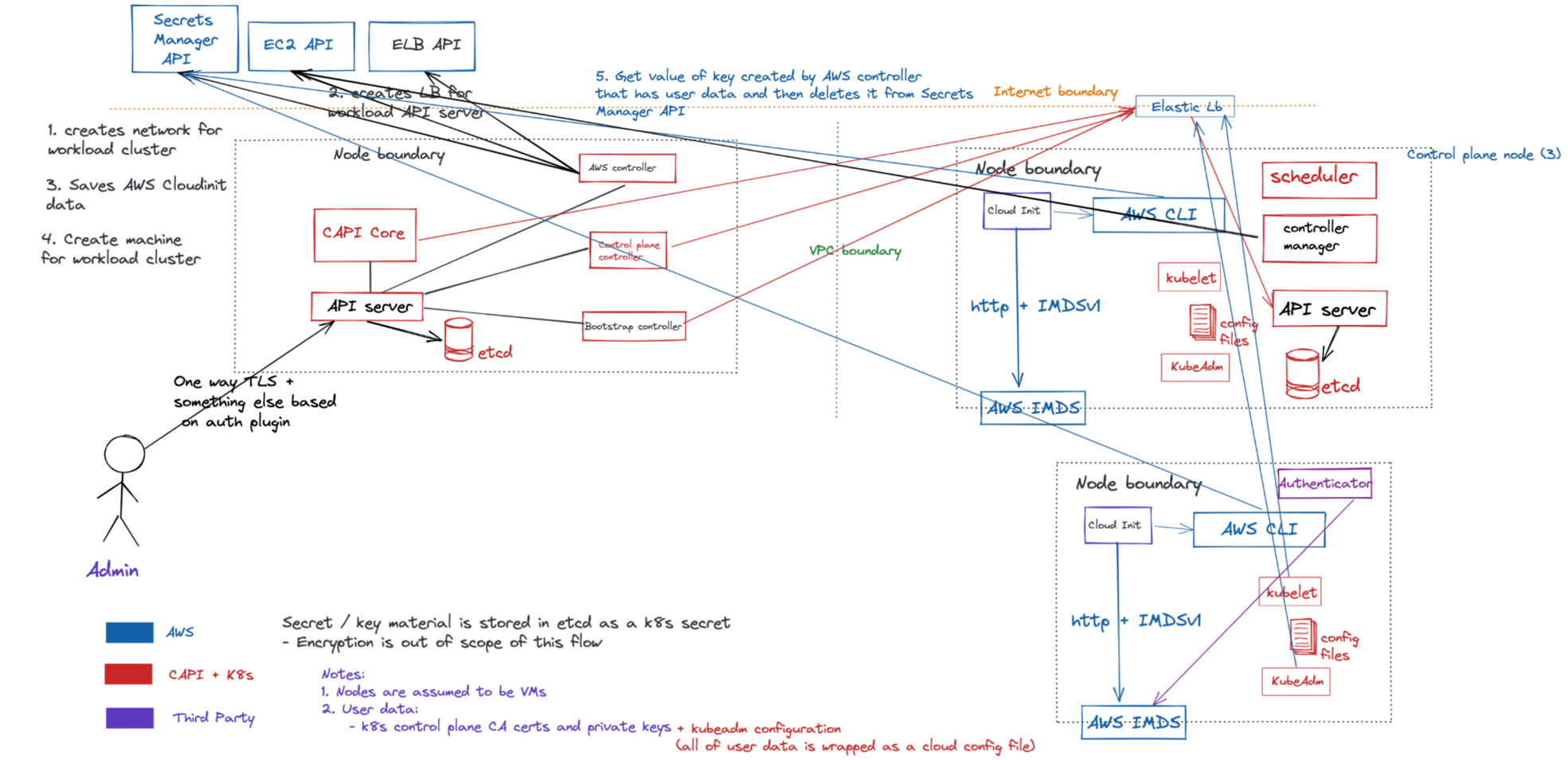
- What workflows are used most?
- What workflows does the community want a security assessment of?

Data Stores and Data flow Diagram (DFD)

Threat Modeling with STRIDE

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service (DoS)
- Elevation of Privilege

DATA FLOW DIAGRAM



github.com/kubernetes/sig-security/blob/main/sig-security-assessments/cluster-api/self-assessment.md

ETCD ASSESSMENT

KubeCon | CloudNativeCon
North America 2025

JOIN TO COLLABORATE!

BUTTERFLY EFFECT

KubeCon | CloudNativeCon
North America 2025

GET INVOLVED!

KubeCon | CloudNativeCon
North America 2025


KubeCon
CloudNativeCon
North America 2025