Service mesh security best practices: from implementation to verification

Anthony Roman, Lei Tang

Google

April 26, 2022

IstioCon

Who are we?

Anthony Roman

Istio

Google Cloud

Github: anthony-roman

Lei Tang

Istio

Google Cloud

Github: lei-tang

IstioCon

Session agenda

1. Service mesh security architecture and implementation.
2. Service mesh security best practices.
3. Lifecycle of service mesh security and demo.

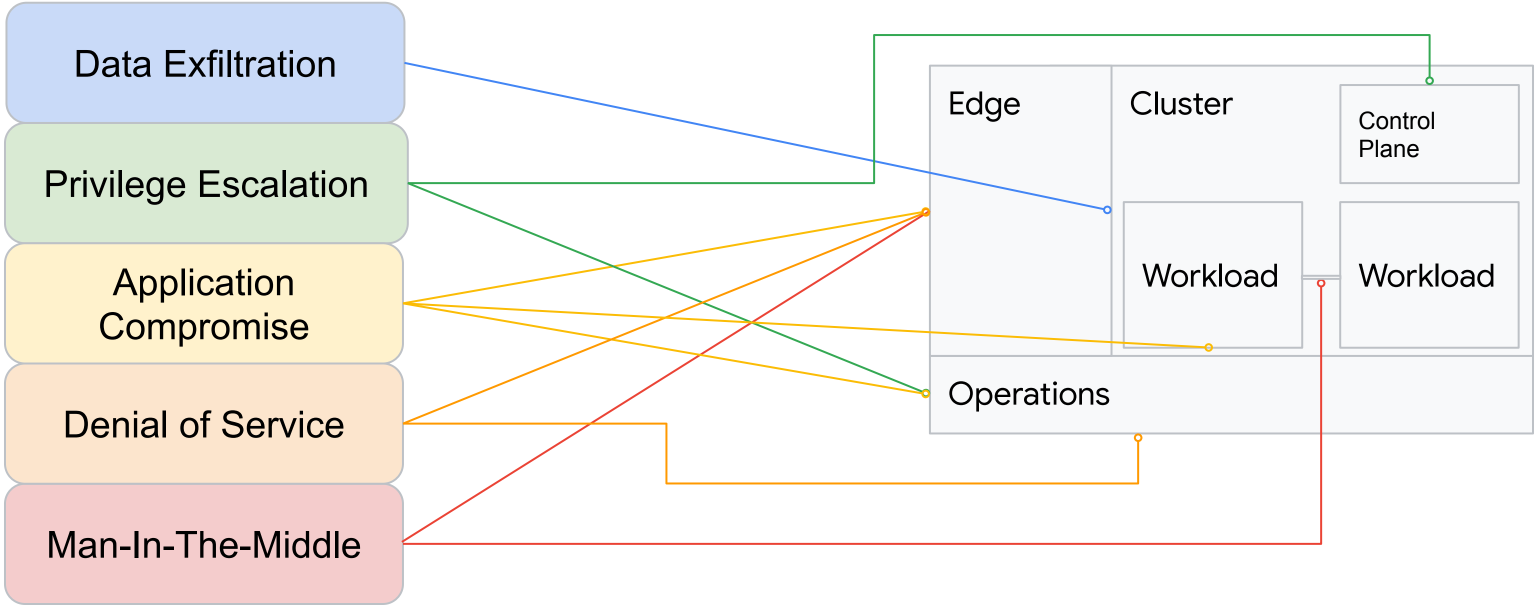
1

Service mesh security architecture

- Attack vectors.
- Service mesh security architecture and implementation.

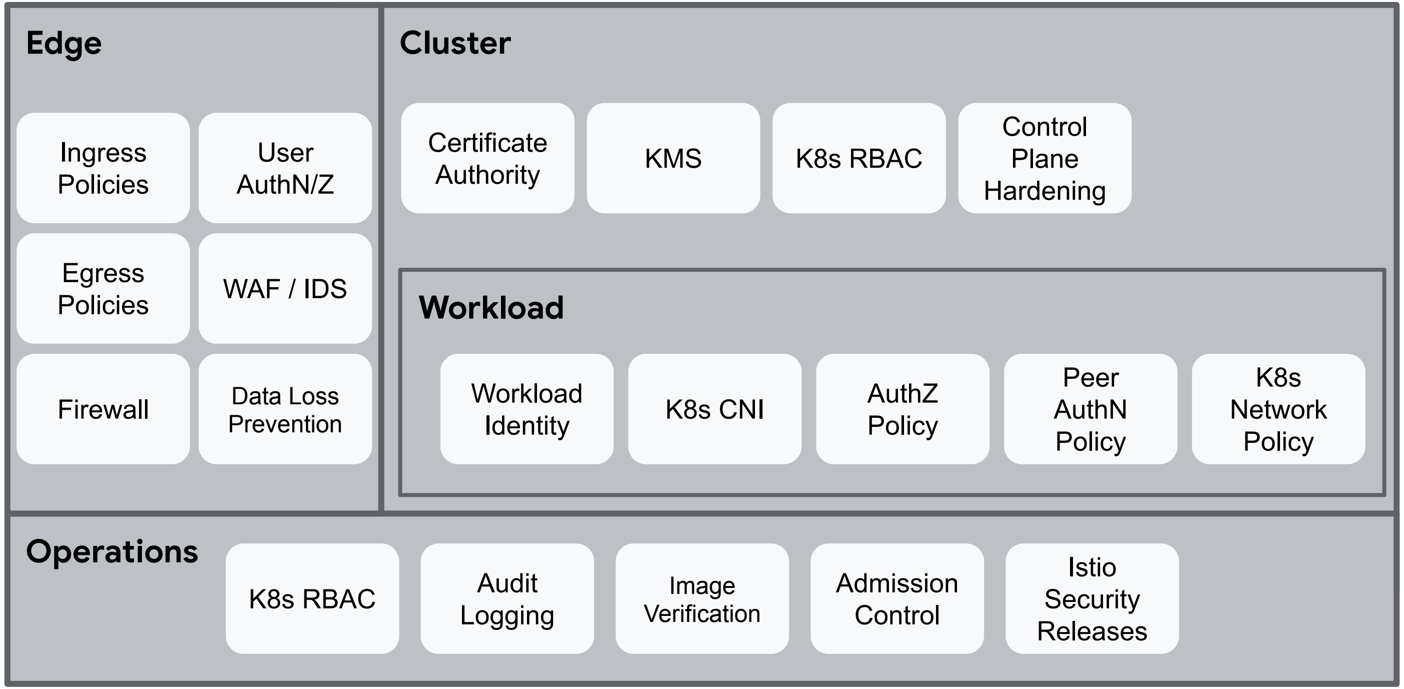
Attack Vectors and Surfaces

Istio is both a collection of security controls and an attack target.



IstioCon

Service mesh security architecture



Edge

- Ingress Policies
- User AuthN/Z
- Egress Policies
- WAF / IDS
- Firewall
- Data Loss Prevention

Cluster

- Certificate Authority
- KMS
- K8s RBAC
- Control Plane Hardening

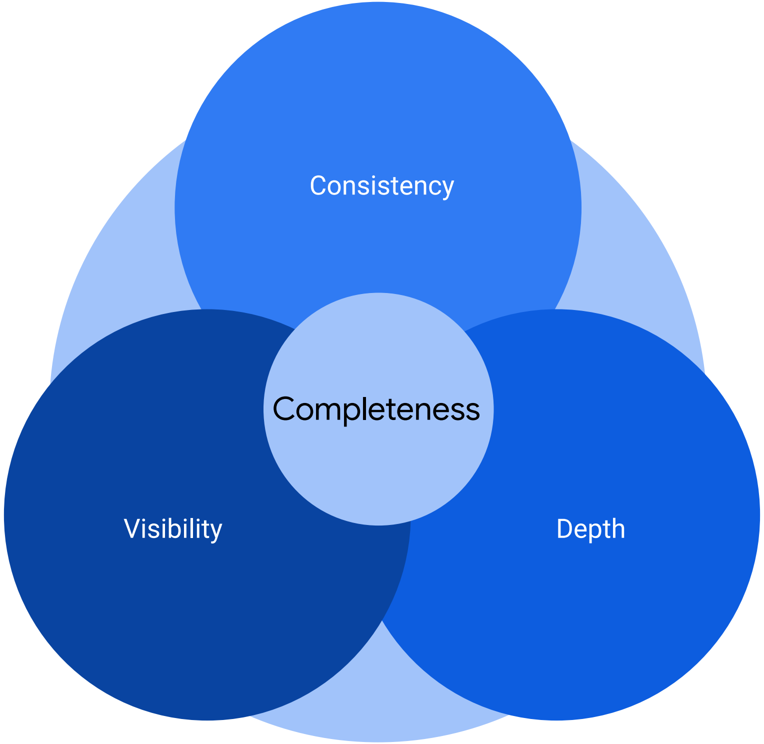
Workload

- Workload Identity
- K8s CNI
- AuthZ Policy
- Peer AuthN Policy
- K8s Network Policy

Operations

- K8s RBAC
- Audit Logging
- Image Verification
- Admission Control
- Istio Security Releases

Complete Security Coverage



Consistency

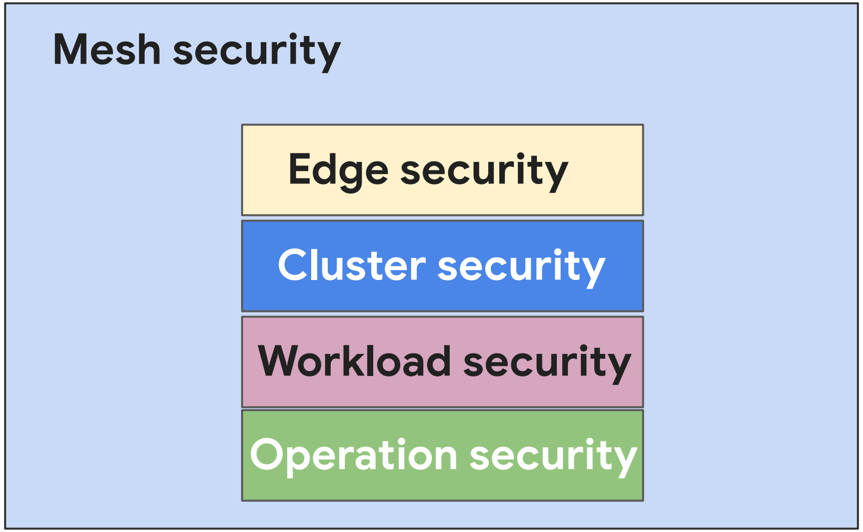
Completeness

Visibility

Depth

2

Service mesh security best practices



Mesh security

Edge security

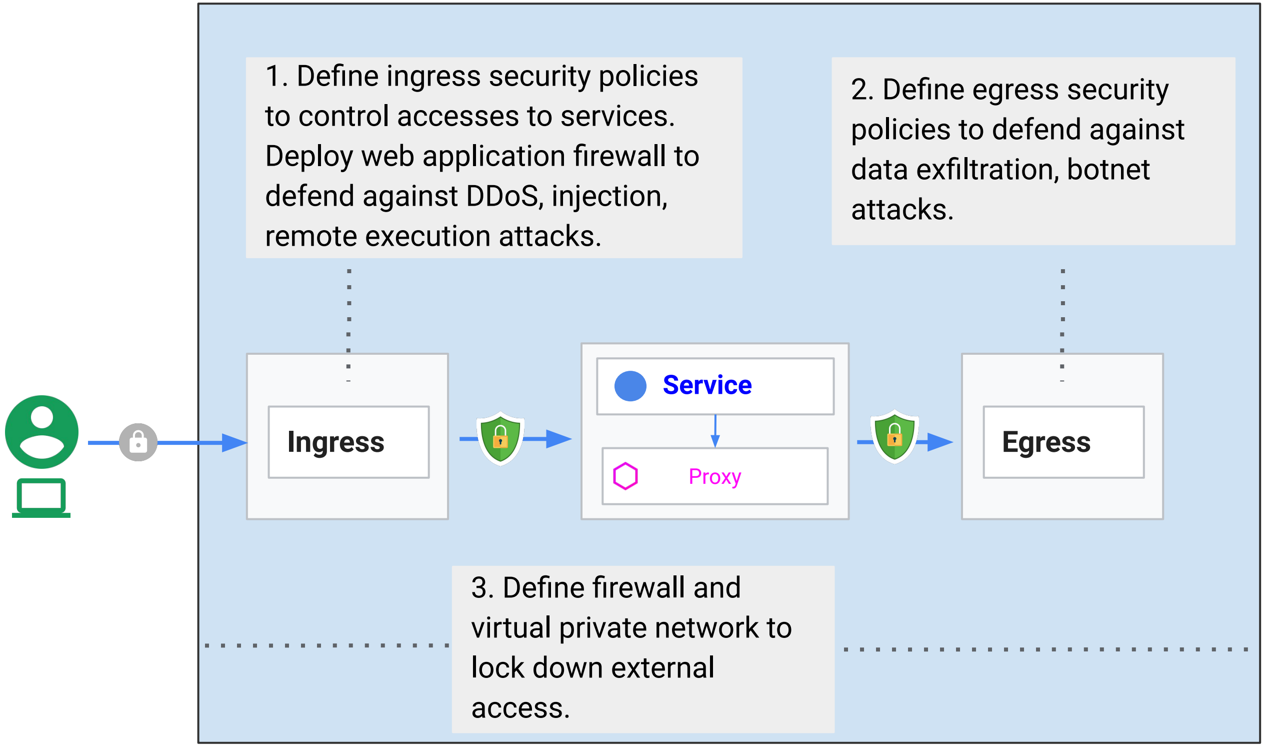
Cluster security

Workload security

Operation security

Edge security best practices

Edge security →

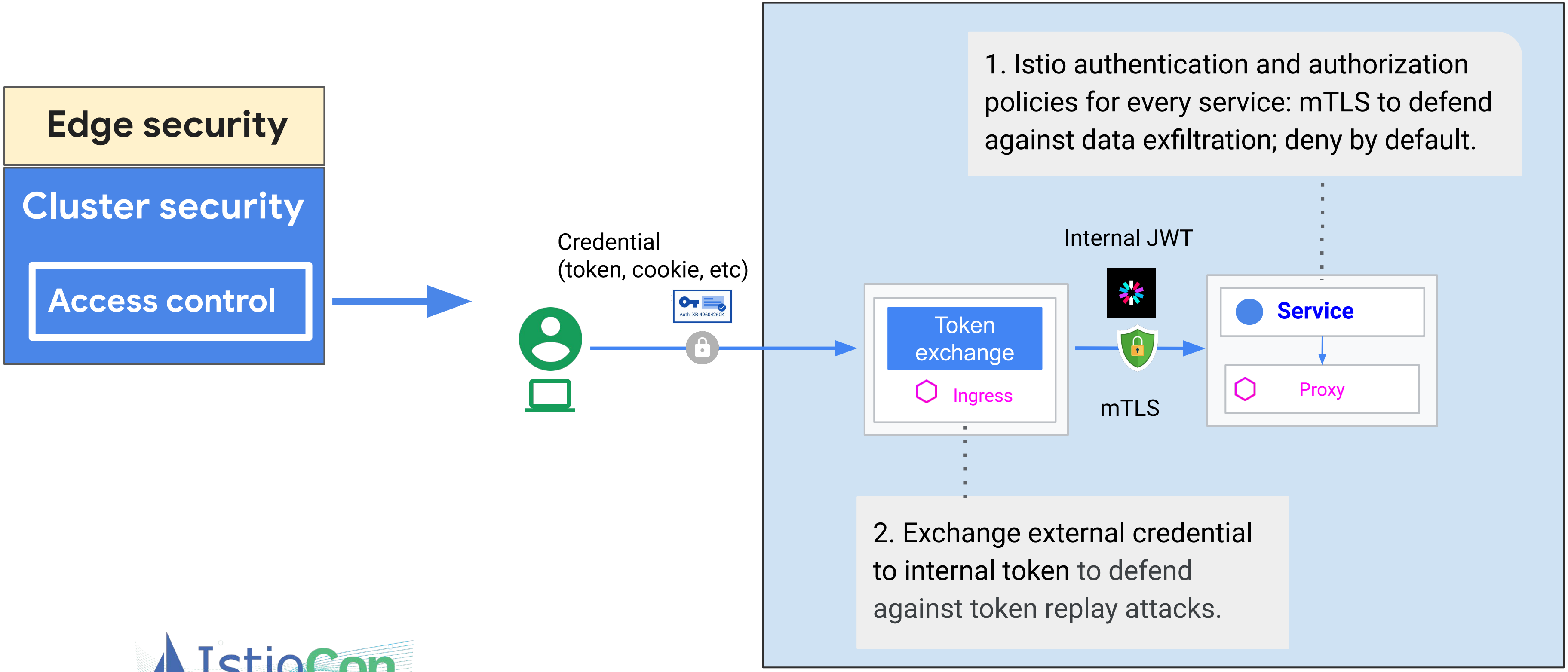


1. Define ingress security policies to control accesses to services. Deploy web application firewall to defend against DDoS, injection, remote execution attacks.

2. Define egress security policies to defend against data exfiltration, botnet attacks.

3. Define firewall and virtual private network to lock down external access.

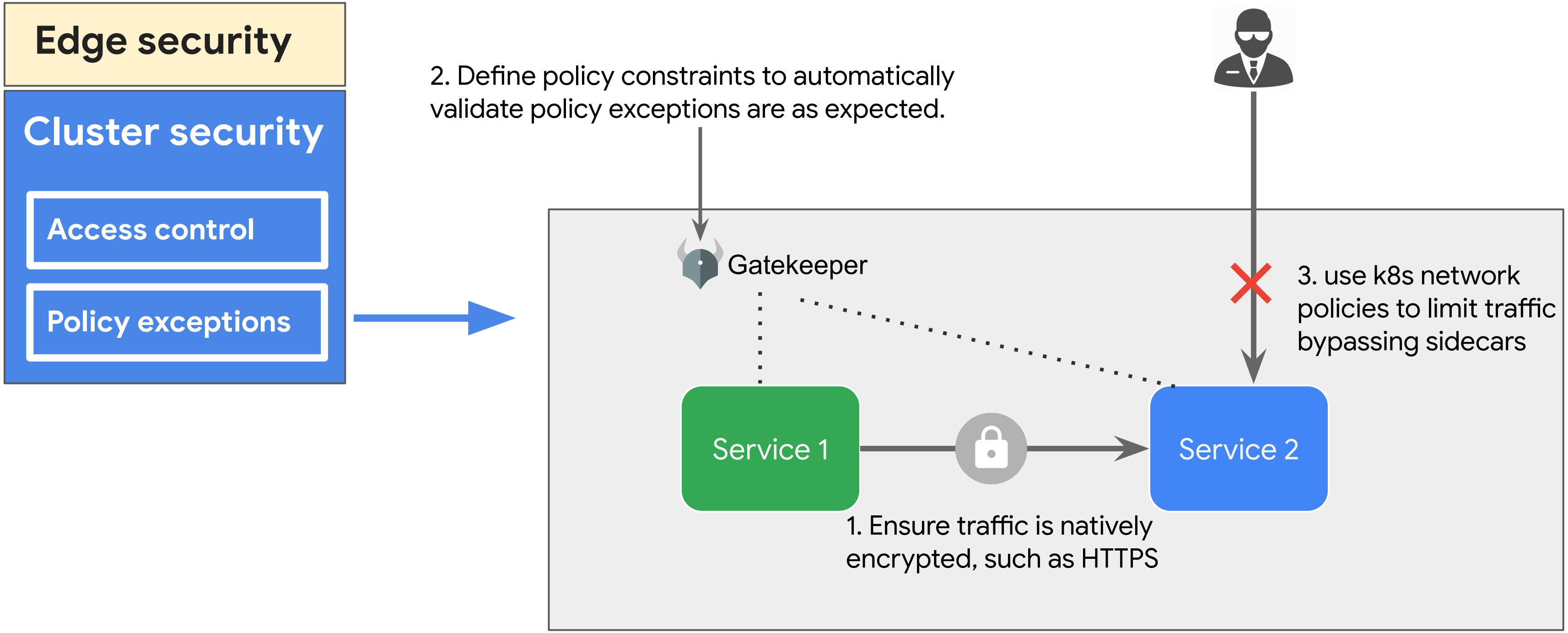
Cluster security best practices: access control



1. Istio authentication and authorization policies for every service: mTLS to defend against data exfiltration; deny by default.

2. Exchange external credential to internal token to defend against token replay attacks.

Cluster security best practices: safely handle policy exceptions



Edge security

Cluster security

Access control

Policy exceptions

2. Define policy constraints to automatically validate policy exceptions are as expected.

Gatekeeper

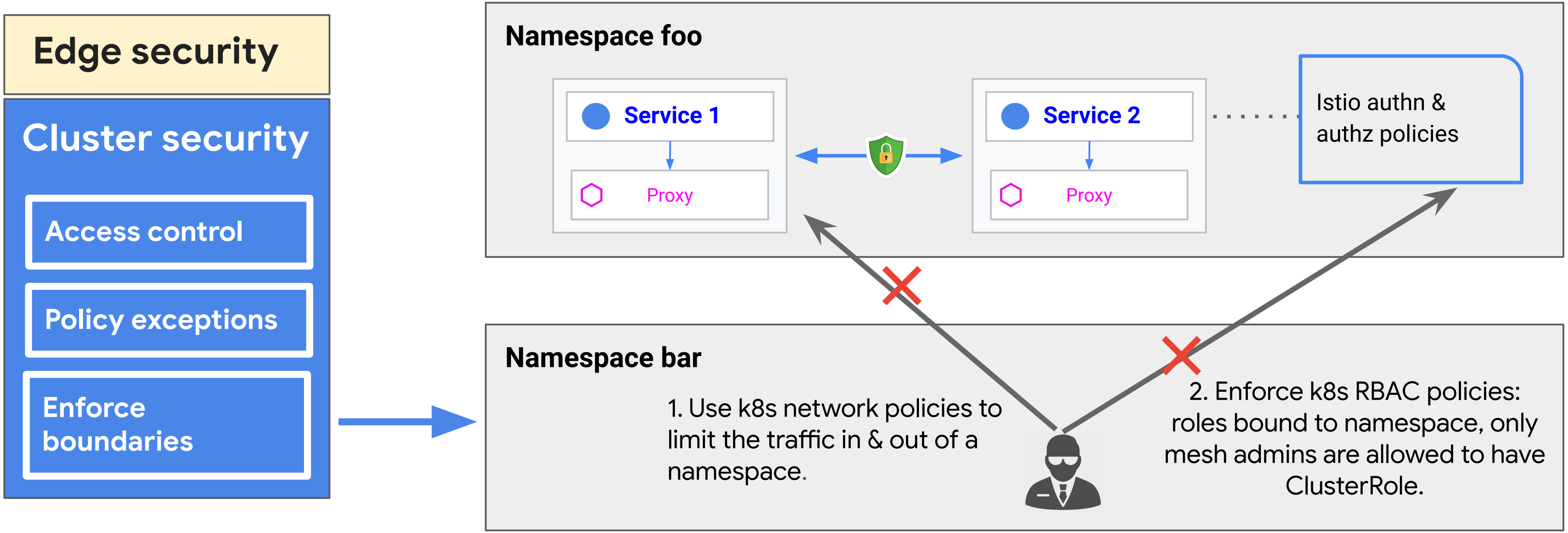
Service 1

Service 2

3. use k8s network policies to limit traffic bypassing sidecars

1. Ensure traffic is natively encrypted, such as HTTPS

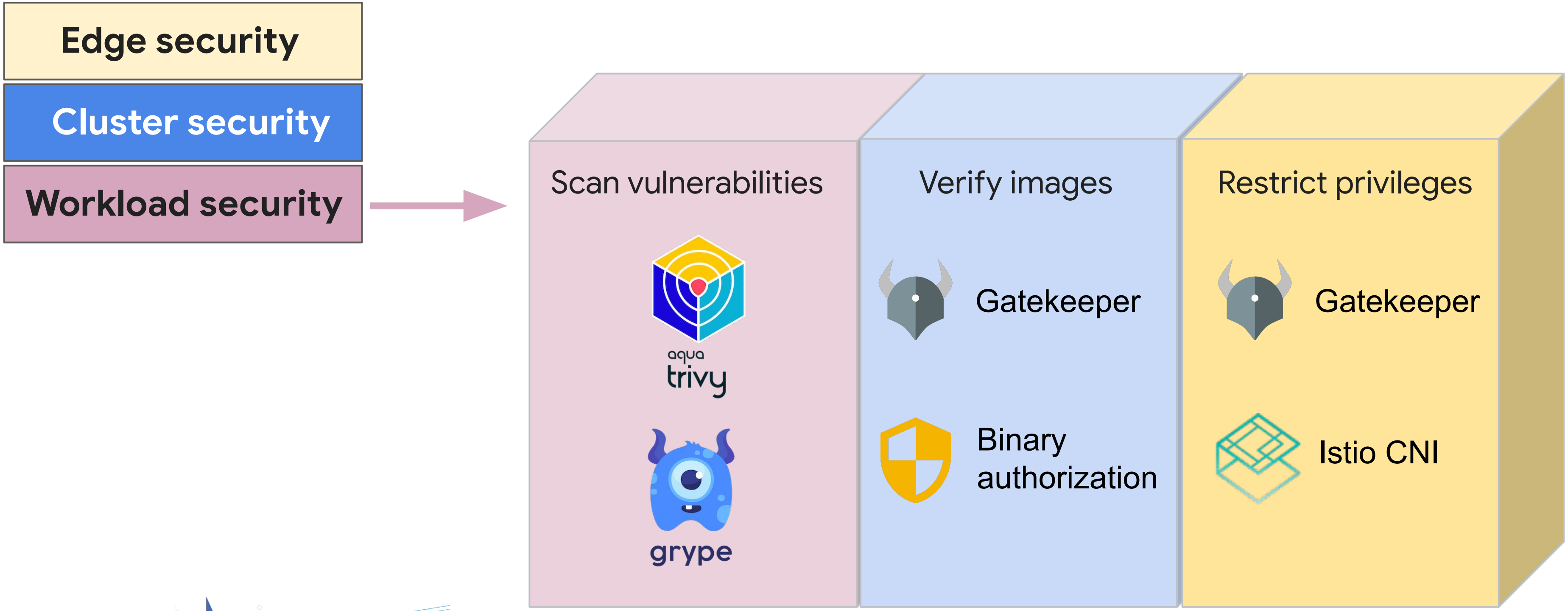
Cluster security best practices: enforce boundaries



1. Use k8s network policies to limit the traffic in & out of a namespace.

2. Enforce k8s RBAC policies: roles bound to namespace, only mesh admins are allowed to have ClusterRole.

Workload security best practices



Edge security

Cluster security

Workload security

Scan vulnerabilities

aqua trivy

grype

Verify images

Gatekeeper

Binary authorization

Restrict privileges

Gatekeeper

Istio CNI

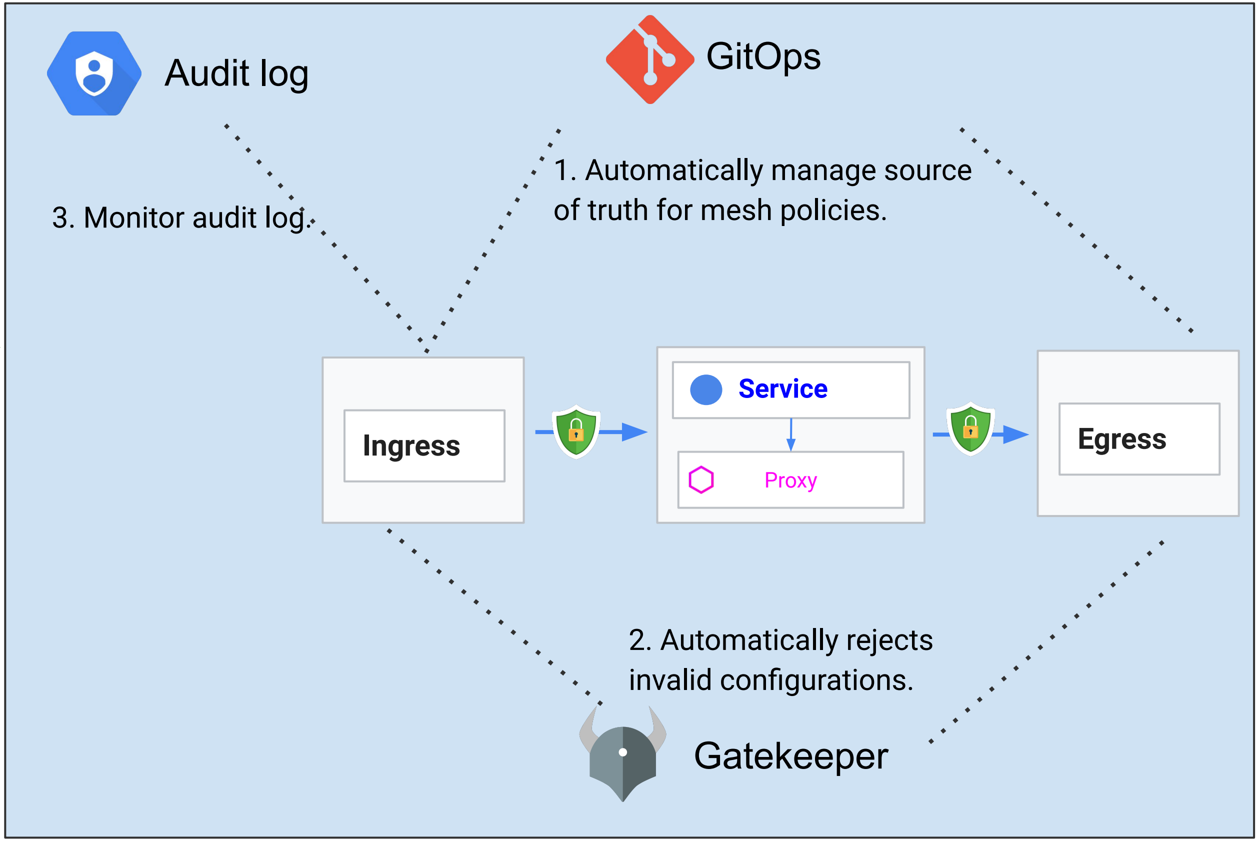
Operation security best practices

Edge security

Cluster security

Workload security

Operation security


Audit log

GitOps

1. Automatically manage source of truth for mesh policies.

2. Automatically rejects invalid configurations.

3. Monitor audit log.

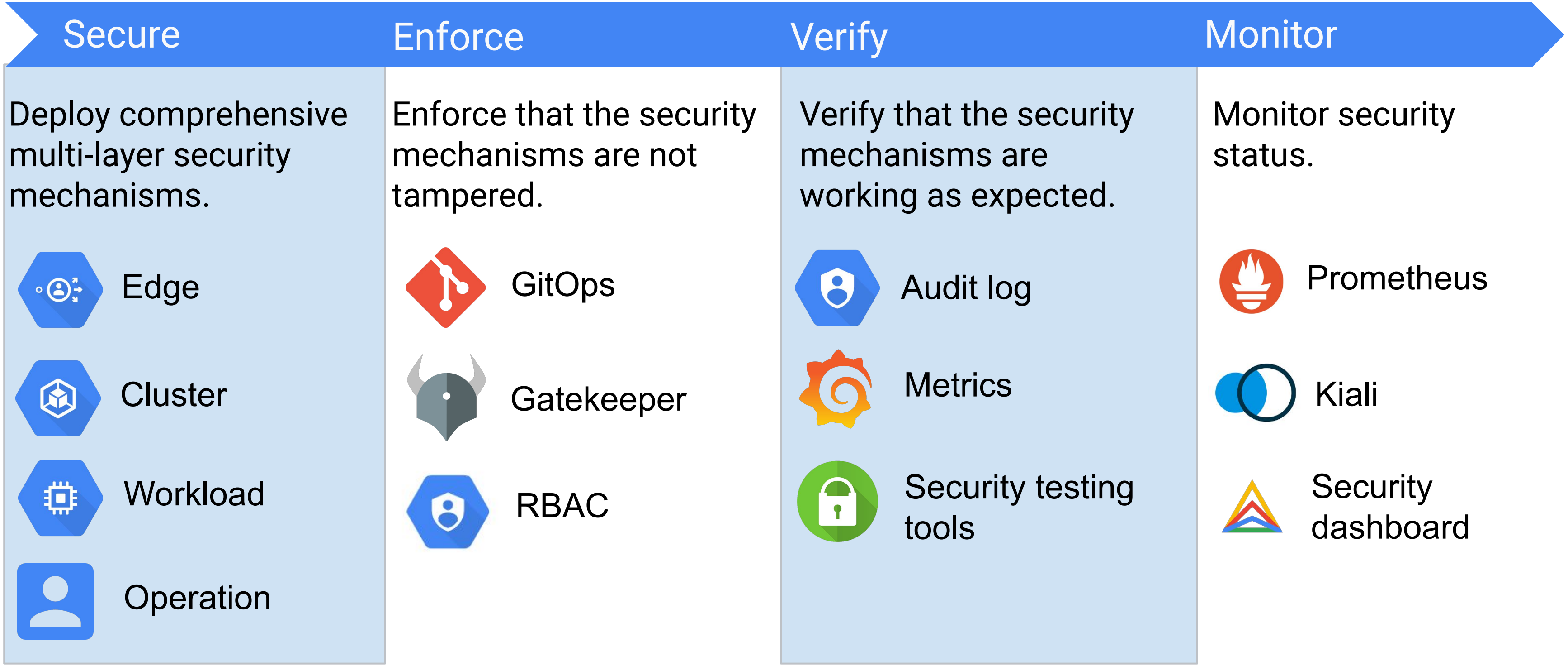
IstioCon

3

Lifecycle of service mesh security and demo

Secure
Enforce
Verify
Monitor

Lifecycle of service mesh security



Secure

Deploy comprehensive multi-layer security mechanisms.

- Edge
- Cluster
- Workload
- Operation

Enforce

Enforce that the security mechanisms are not tampered.

- GitOps
- Gatekeeper
- RBAC

Verify

Verify that the security mechanisms are working as expected.

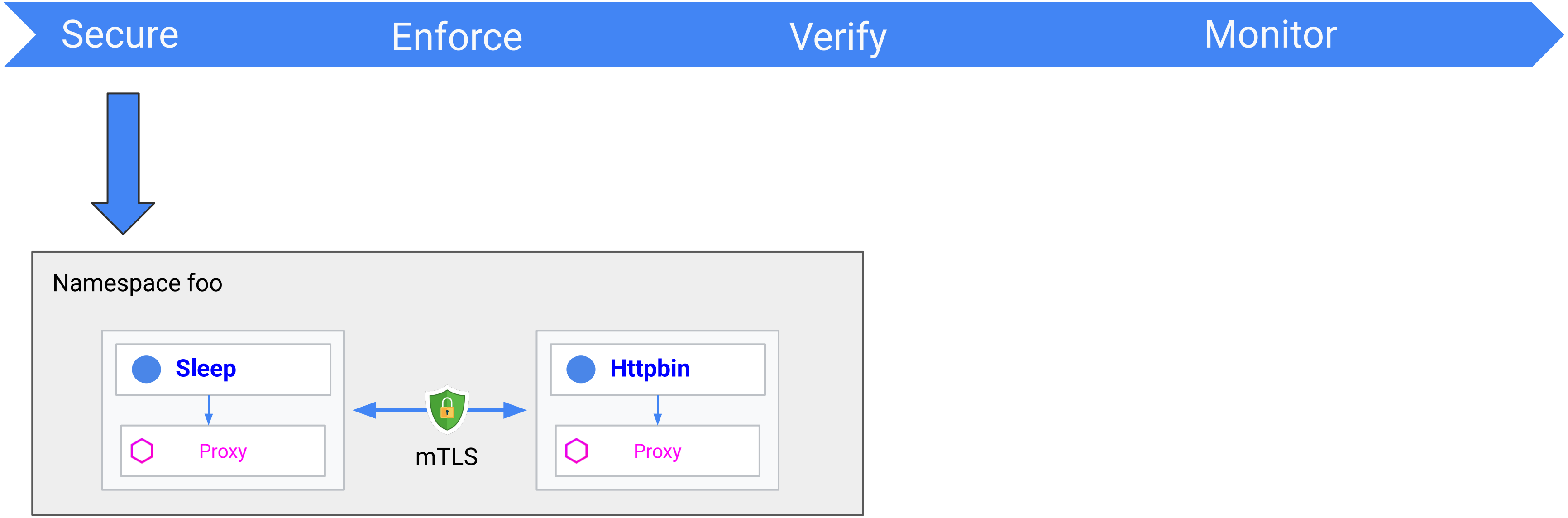
- Audit log
- Metrics
- Security testing tools

Monitor

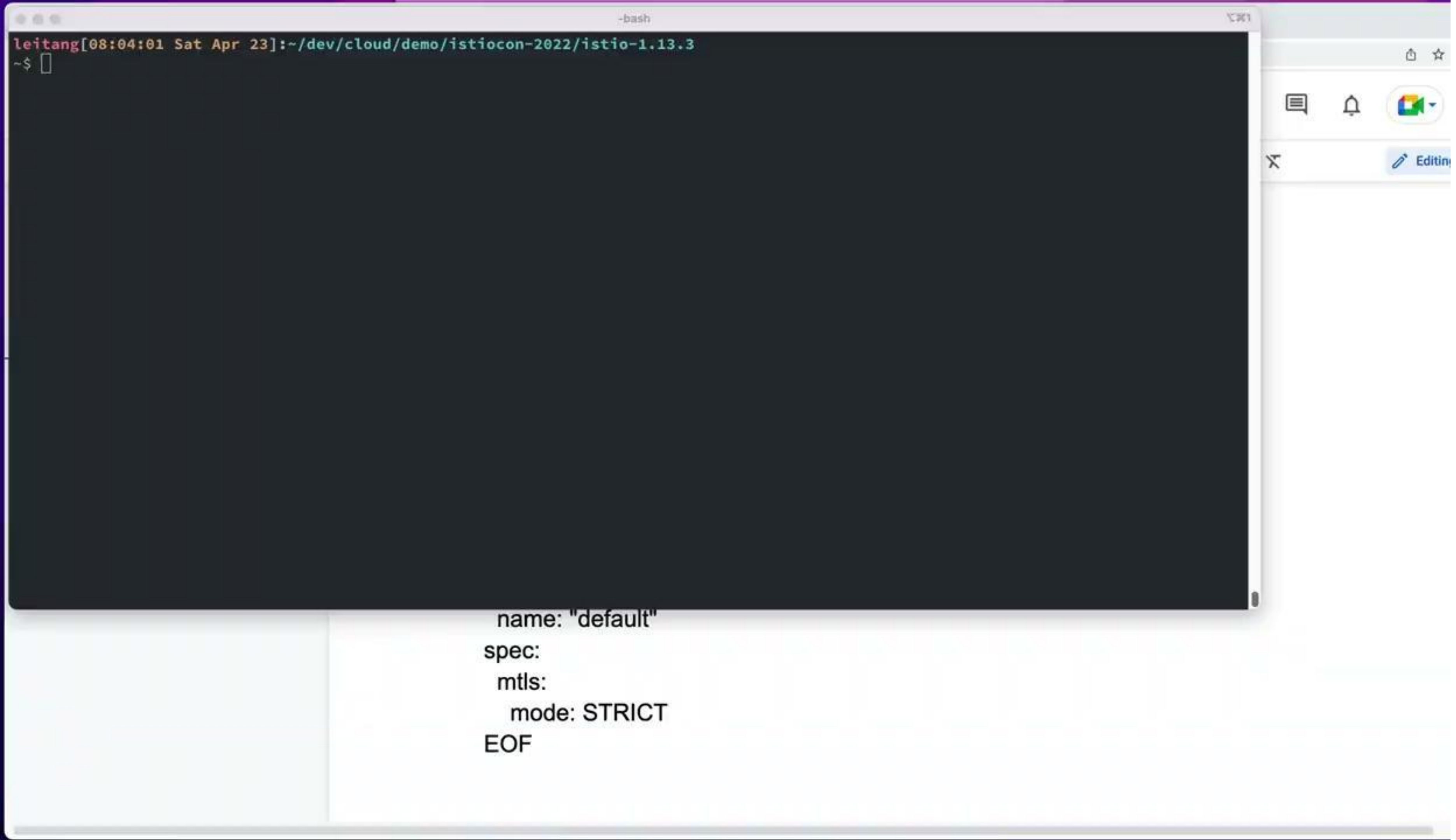
Monitor security status.

- Prometheus
- Kiali
- Security dashboard

Demo: mesh security lifecycle



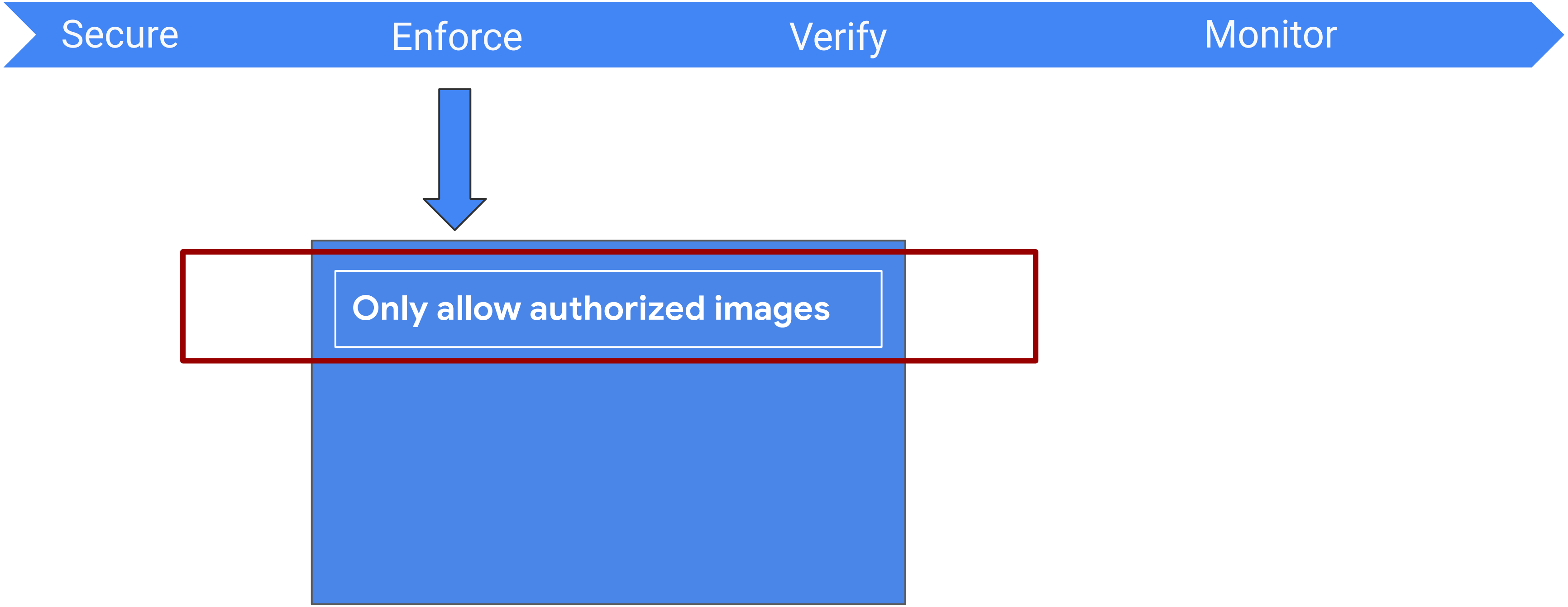
Demo



```
leitang[08:04:01 Sat Apr 23]:~/dev/cloud/demo/istiocon-2022/istio-1.13.3
~$ 
```

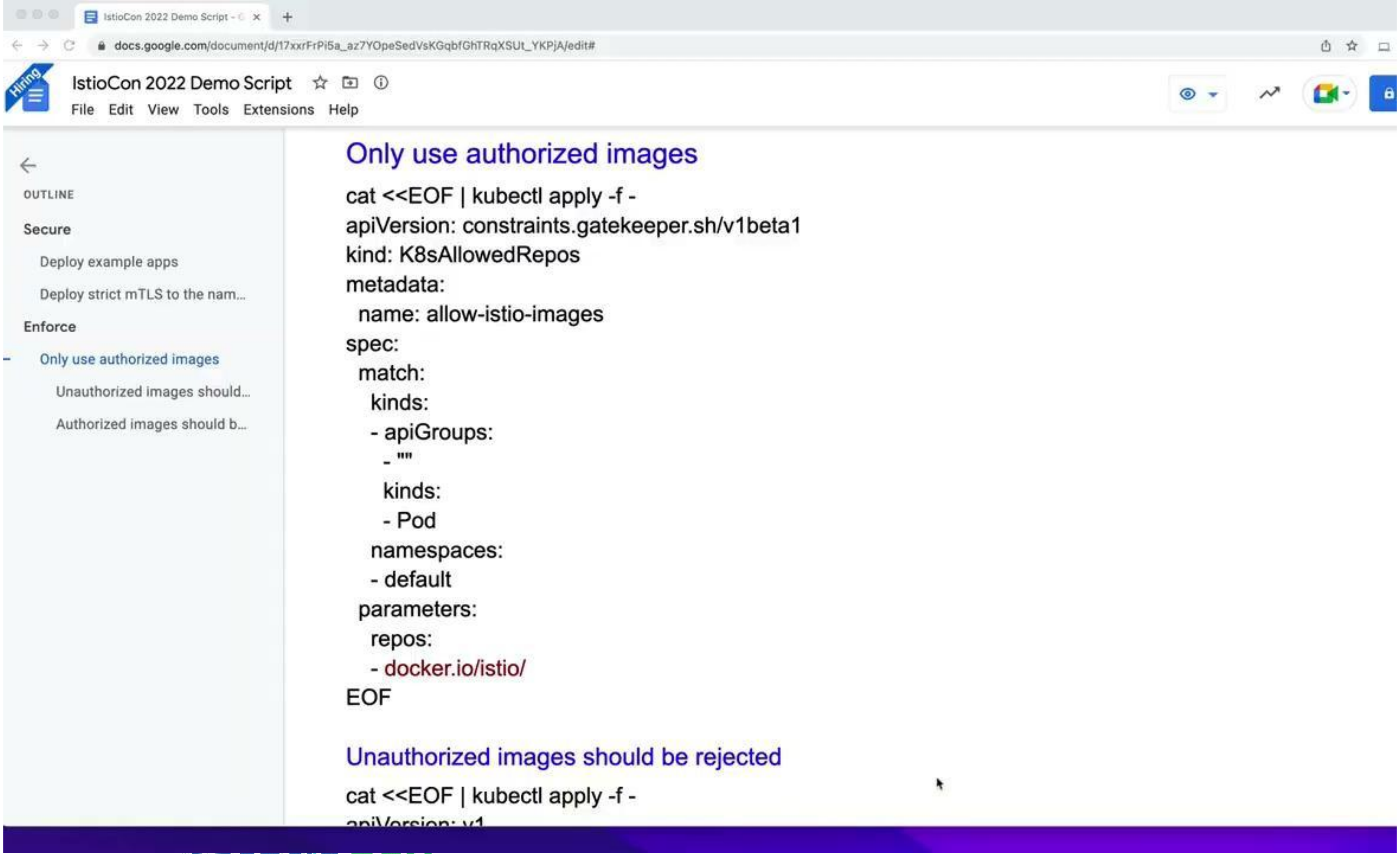
```
  name: "default"
spec:
  mtls:
    mode: STRICT
EOF
```

Demo: mesh security lifecycle



IstioCon

Demo


IstioCon 2022 Demo Script - G
docs.google.com/document/d/17xxrFrPi5a_az7YOpeSedVsKGqbfGhTRqXSUt_YKPjA/edit#
IstioCon 2022 Demo Script
File Edit View Tools Extensions Help
OUTLINE
Secure
Deploy example apps
Deploy strict mTLS to the nam...
Enforce
Only use authorized images
Unauthorized images should...
Authorized images should b...

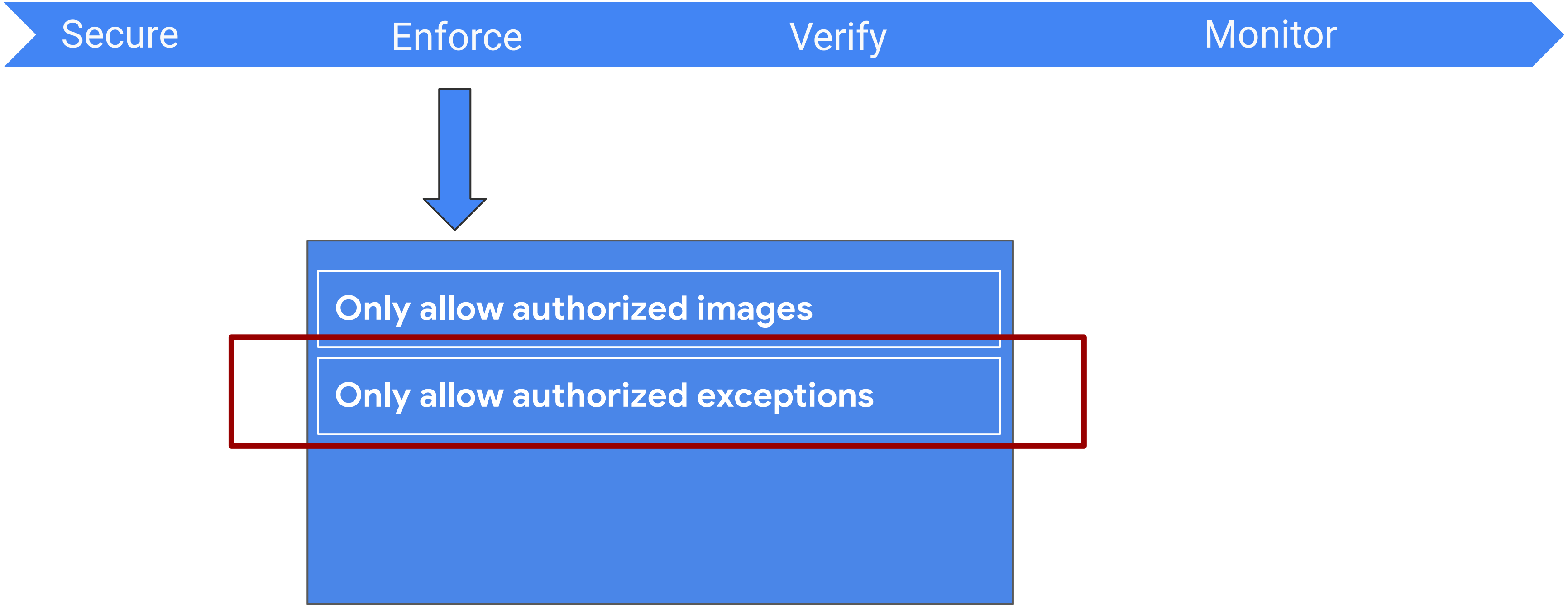
Only use authorized images

```
cat <<EOF | kubectl apply -f -
apiVersion: constraints.gatekeeper.sh/v1beta1
kind: K8sAllowedRepos
metadata:
  name: allow-istio-images
spec:
  match:
    kinds:
    - apiGroups:
      - ""
      kinds:
      - Pod
    namespaces:
    - default
  parameters:
    repos:
    - docker.io/istio/
EOF
```

Unauthorized images should be rejected

```
cat <<EOF | kubectl apply -f -
apiVersion: v1
```

Demo: mesh security lifecycle



Secure

Enforce

Verify

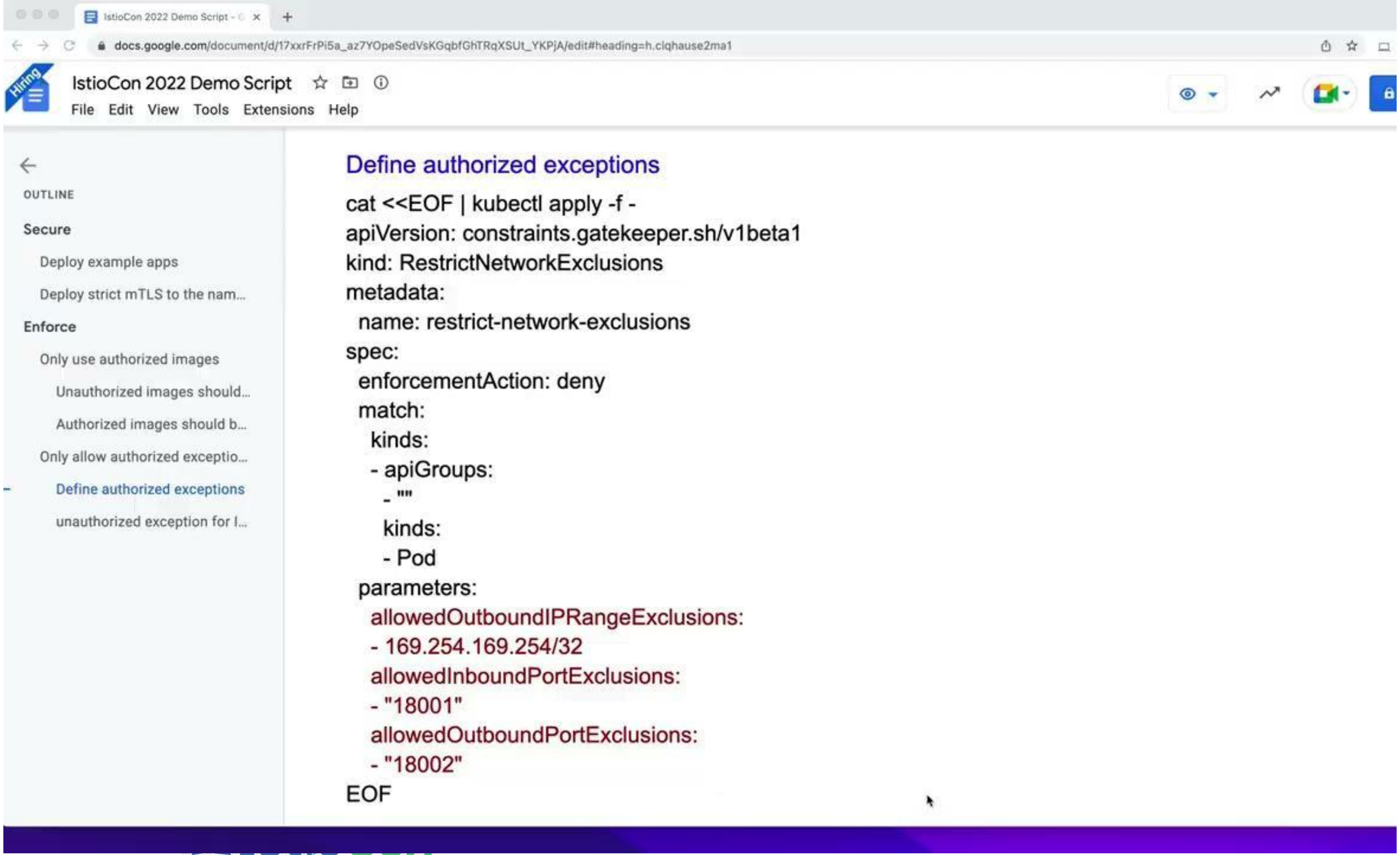
Monitor

Only allow authorized images

Only allow authorized exceptions

IstioCon

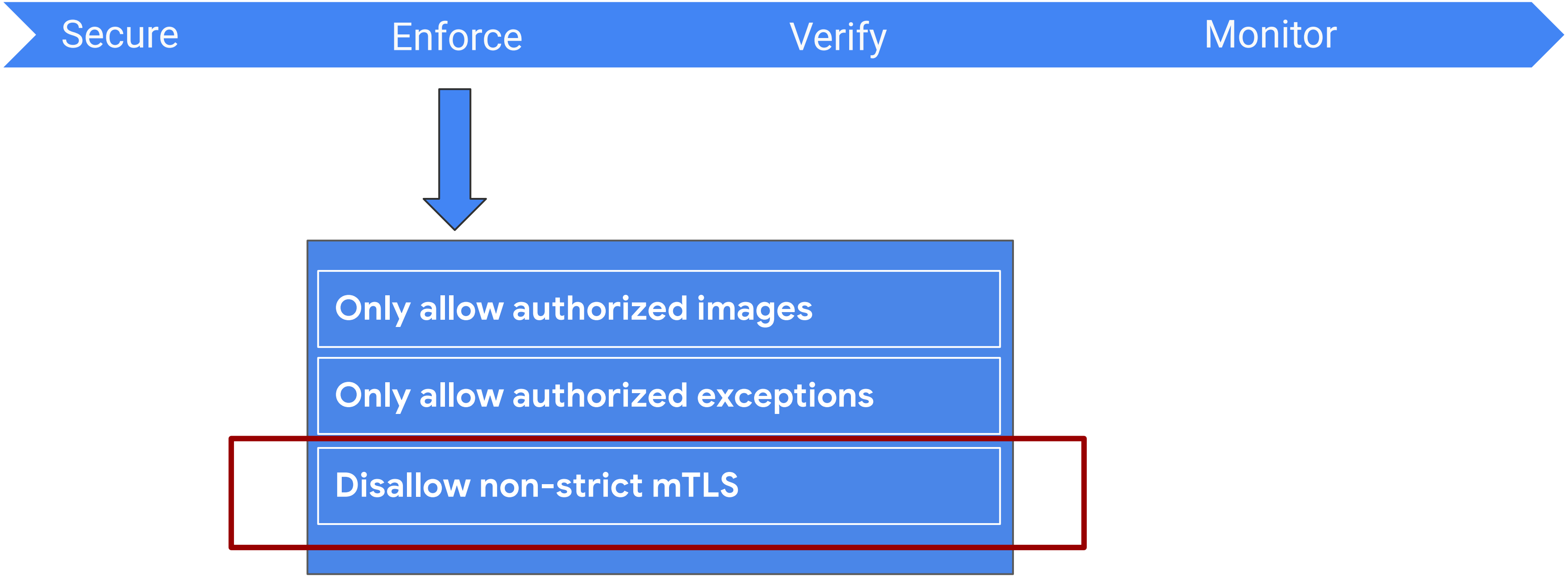
Demo


IstioCon 2022 Demo Script
docs.google.com/document/d/17xxrFrPi5a_az7YOpeSedVsKGqbfGhTRqXSUt_YKPjA/edit#heading=h.clqhause2ma1
IstioCon 2022 Demo Script
File
Edit
View
Tools
Extensions
Help
OUTLINE
Secure
Deploy example apps
Deploy strict mTLS to the nam...
Enforce
Only use authorized images
Unauthorized images should...
Authorized images should b...
Only allow authorized exceptio...
Define authorized exceptions
unauthorized exception for I...

Define authorized exceptions

```
cat <<EOF | kubectl apply -f -
apiVersion: constraints.gatekeeper.sh/v1beta1
kind: RestrictNetworkExclusions
metadata:
  name: restrict-network-exclusions
spec:
  enforcementAction: deny
  match:
    kinds:
    - apiGroups:
      - ""
      kinds:
      - Pod
  parameters:
    allowedOutboundIPRangeExclusions:
    - 169.254.169.254/32
    allowedInboundPortExclusions:
    - "18001"
    allowedOutboundPortExclusions:
    - "18002"
EOF
```

Demo: mesh security lifecycle



Secure

Enforce

Verify

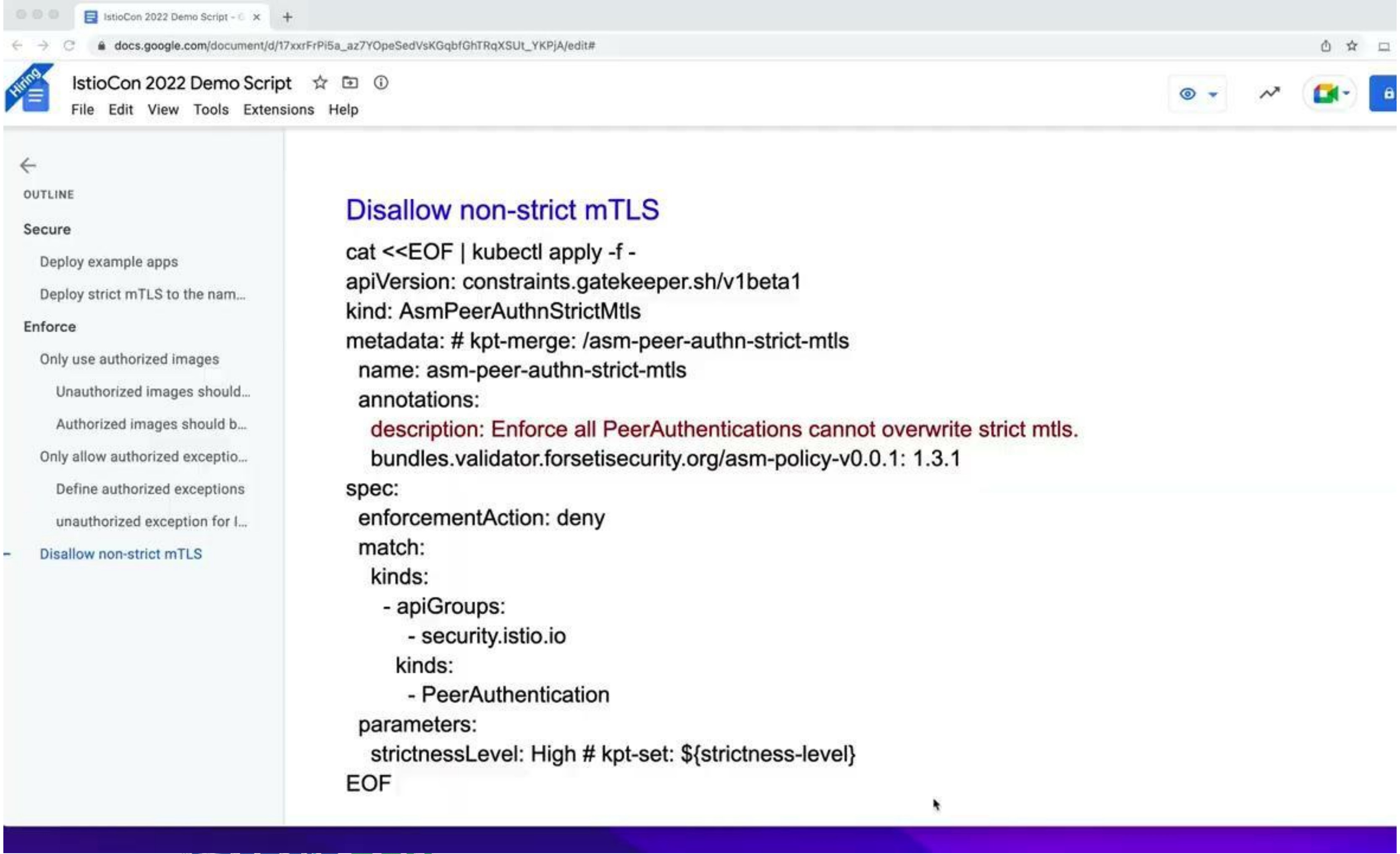
Monitor

Only allow authorized images

Only allow authorized exceptions

Disallow non-strict mTLS

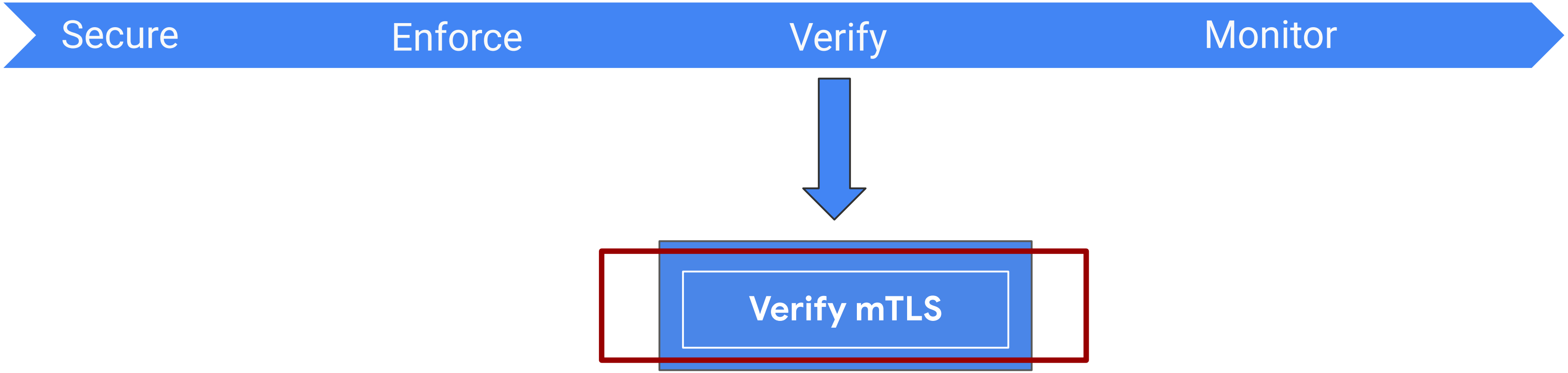
Demo


IstioCon 2022 Demo Script - G
docs.google.com/document/d/17xxrFrPi5a_az7YOpeSedVsKGqbfGhTRqXSUt_YKPjA/edit#
IstioCon 2022 Demo Script
File
Edit
View
Tools
Extensions
Help
OUTLINE
Secure
Deploy example apps
Deploy strict mTLS to the nam...
Enforce
Only use authorized images
Unauthorized images should...
Authorized images should b...
Only allow authorized exceptio...
Define authorized exceptions
unauthorized exception for I...
Disallow non-strict mTLS

Disallow non-strict mTLS

```
cat <<EOF | kubectl apply -f -
apiVersion: constraints.gatekeeper.sh/v1beta1
kind: AsmPeerAuthnStrictMtls
metadata: # kpt-merge: /asm-peer-authn-strict-mtls
  name: asm-peer-authn-strict-mtls
  annotations:
    description: Enforce all PeerAuthentications cannot overwrite strict mtls.
    bundles.validator.forsetisecurity.org/asm-policy-v0.0.1: 1.3.1
spec:
  enforcementAction: deny
  match:
    kinds:
      - apiGroups:
          - security.istio.io
        kinds:
          - PeerAuthentication
  parameters:
    strictnessLevel: High # kpt-set: ${strictness-level}
EOF
```

Demo: mesh security lifecycle



Secure

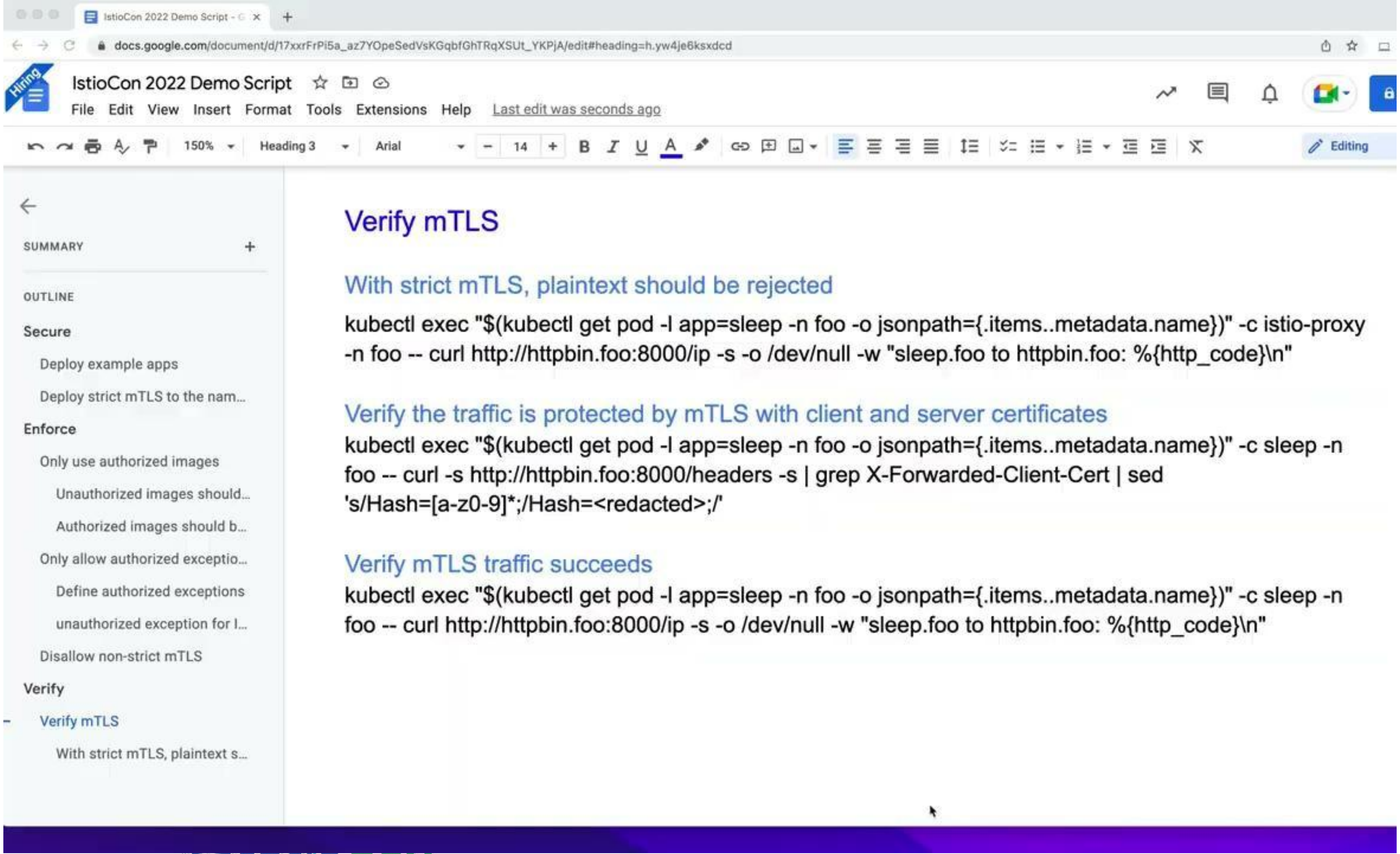
Enforce

Verify

Monitor

Verify mTLS

Demo



IstioCon 2022 Demo Script - G
docs.google.com/document/d/17xxrFrPi5a_az7YOpeSedVsKGqbfGhTRqXSUt_YKPjA/edit#heading=h.yw4je6ksxdcd
IstioCon 2022 Demo Script
File
Edit
View
Insert
Format
Tools
Extensions
Help
Last edit was seconds ago
150%
Heading 3
Arial
14
Editing
SUMMARY
OUTLINE
Secure
Deploy example apps
Deploy strict mTLS to the nam...
Enforce
Only use authorized images
Unauthorized images should...
Authorized images should b...
Only allow authorized exceptio...
Define authorized exceptions
unauthorized exception for l...
Disallow non-strict mTLS
Verify
Verify mTLS
With strict mTLS, plaintext s...

Verify mTLS

With strict mTLS, plaintext should be rejected

```
kubectl exec "$(kubectl get pod -l app=sleep -n foo -o jsonpath={.items..metadata.name})" -c istio-proxy -n foo -- curl http://httpbin.foo:8000/ip -s -o /dev/null -w "sleep.foo to httpbin.foo: %{http_code}\n"
```

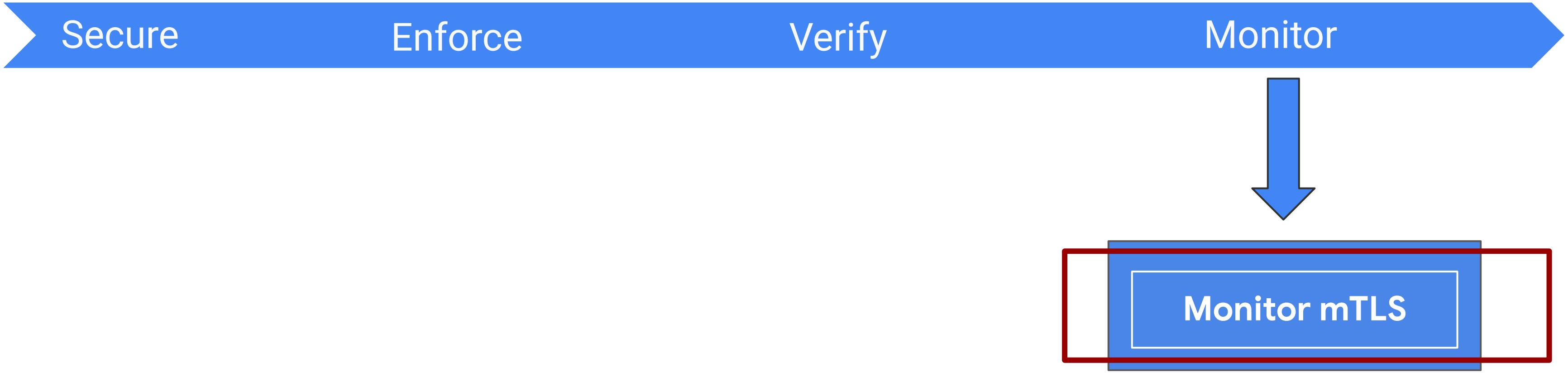
Verify the traffic is protected by mTLS with client and server certificates

```
kubectl exec "$(kubectl get pod -l app=sleep -n foo -o jsonpath={.items..metadata.name})" -c sleep -n foo -- curl -s http://httpbin.foo:8000/headers -s | grep X-Forwarded-Client-Cert | sed 's/Hash=[a-z0-9]*;/Hash=<redacted>;/'
```

Verify mTLS traffic succeeds

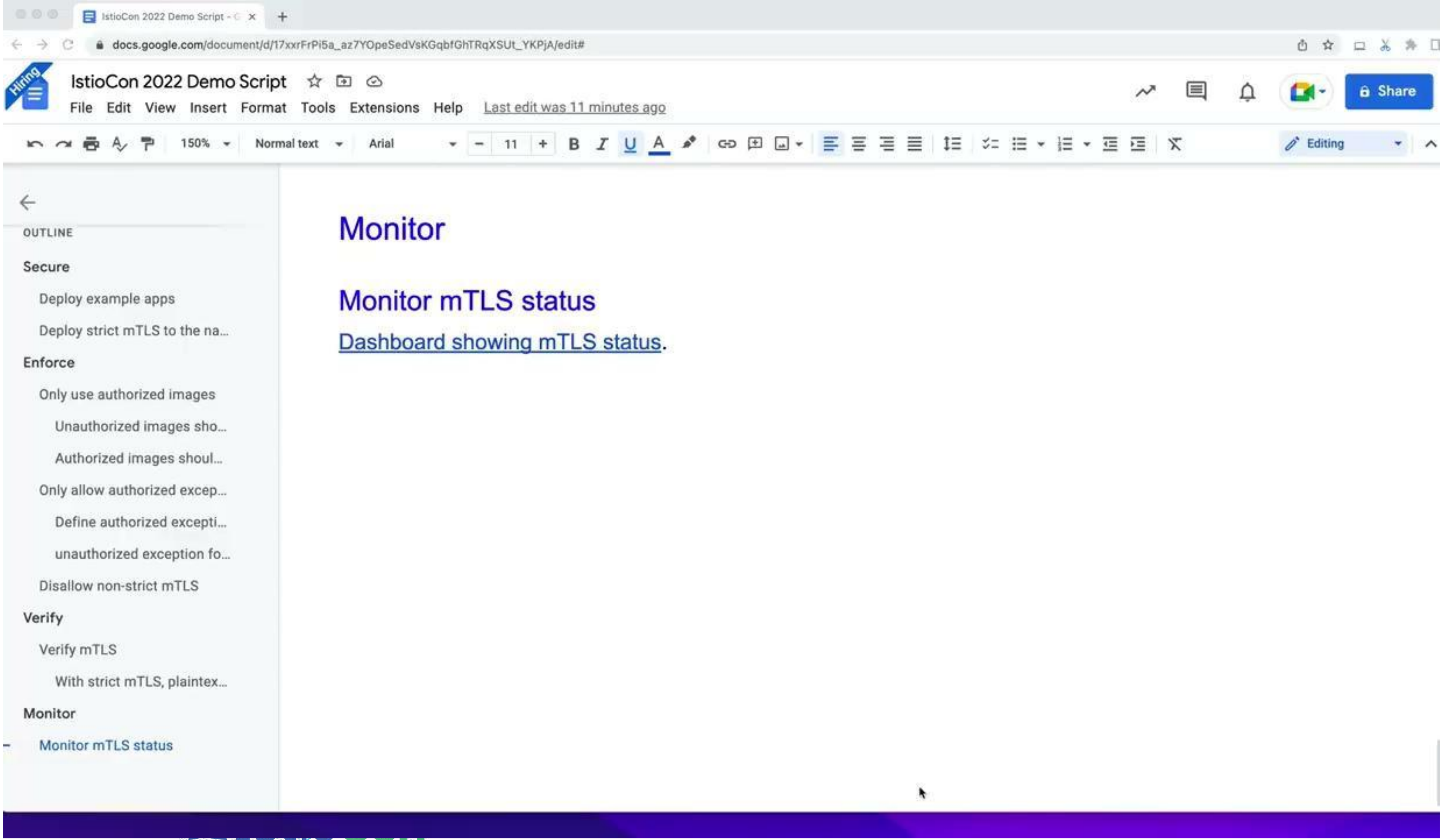
```
kubectl exec "$(kubectl get pod -l app=sleep -n foo -o jsonpath={.items..metadata.name})" -c sleep -n foo -- curl http://httpbin.foo:8000/ip -s -o /dev/null -w "sleep.foo to httpbin.foo: %{http_code}\n"
```

Demo: mesh security lifecycle



IstioCon

Demo


IstioCon 2022 Demo Script - G
docs.google.com/document/d/17xxrFrPi5a_az7YOpeSedVsKGqbfGhTRqXSUt_YKPjA/edit#
IstioCon 2022 Demo Script
File
Edit
View
Insert
Format
Tools
Extensions
Help
Last edit was 11 minutes ago
Share
150%
Normal text
Arial
11
Editing

OUTLINE

Secure
- Deploy example apps
- Deploy strict mTLS to the na...

Enforce
- Only use authorized images
  - Unauthorized images sho...
  - Authorized images shoul...
- Only allow authorized excep...
  - Define authorized excepti...
  - unauthorized exception fo...
- Disallow non-strict mTLS

Verify
- Verify mTLS
  - With strict mTLS, plaintex...

Monitor
- Monitor mTLS status

Monitor

Monitor mTLS status

Dashboard showing mTLS status.

Thank You!

Resources:

- https://istio.io/latest/docs/ops/best-practices/security/
- https://cloud.google.com/service-mesh/docs/security/anthos-service-mesh-security-best-practices