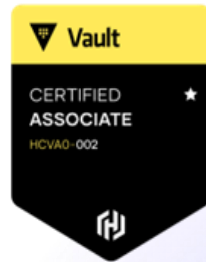


SECURING KUBERNETES ACROSS THE STACK

SHINEBAYAR .TS, Senior cloud native architect

DLP LLC



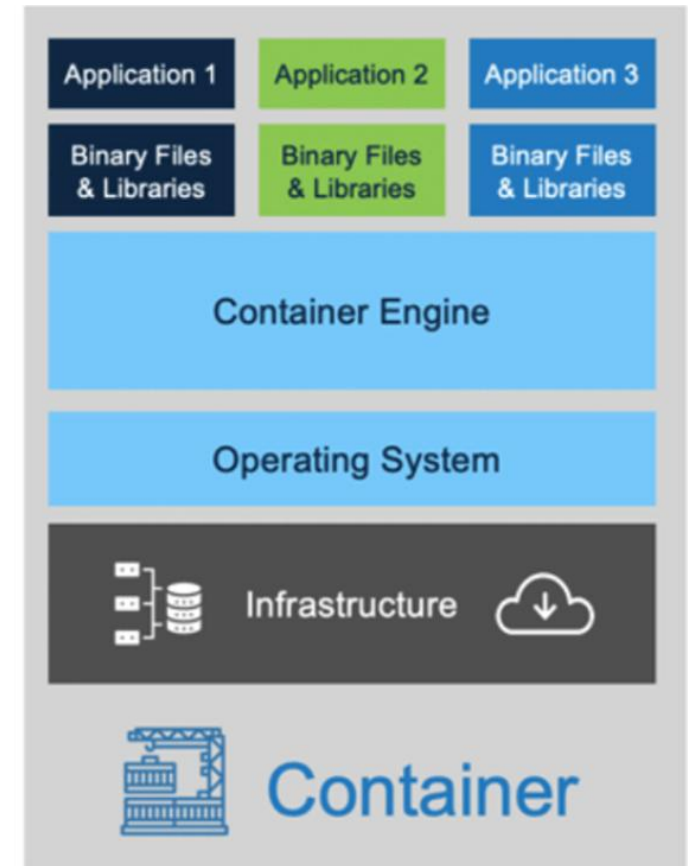
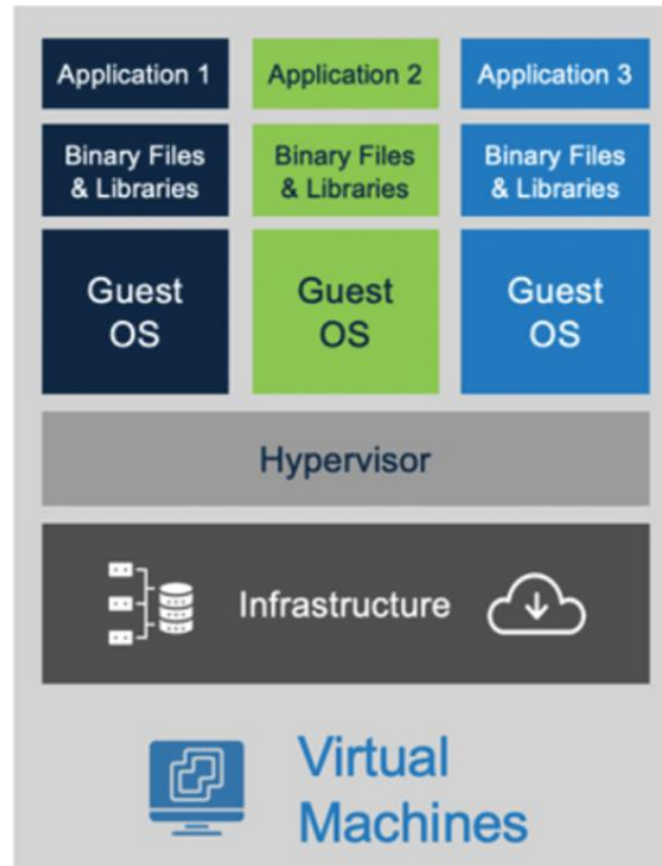
ABOUT ME



AGENDA

- What is a Container & Kubernetes ?
- Why Kubernetes security matters ?
- Layers of Kubernetes security
- Supply Chain Attack
- Disaster Recovery
- Useful tools
- Q&A

WHAT IS A CONTAINER ?



WHAT IS KUBERNETES ?



WHY KUBERNETES SECURITY MATTERS

What Are Your Challenges In Using / Deploying Containers?

Segmented By Extent Organization Has Adopted Cloud Native Technologies



SECURITY IS #1 CHALLENGE FOR PRODUCTION CONTAINERS

- Lack of training is the top challenge for organizations adopting containers.
- Security is the top challenge for organizations running containers in production for two years in a row.

WHY KUBERNETES SECURITY MATTERS

Real-World Security Cases:

1. “RBAC Buster”

- Cryptomining & Persistent Backdoors
- Impacted 60+ clusters due to misconfigured RBAC

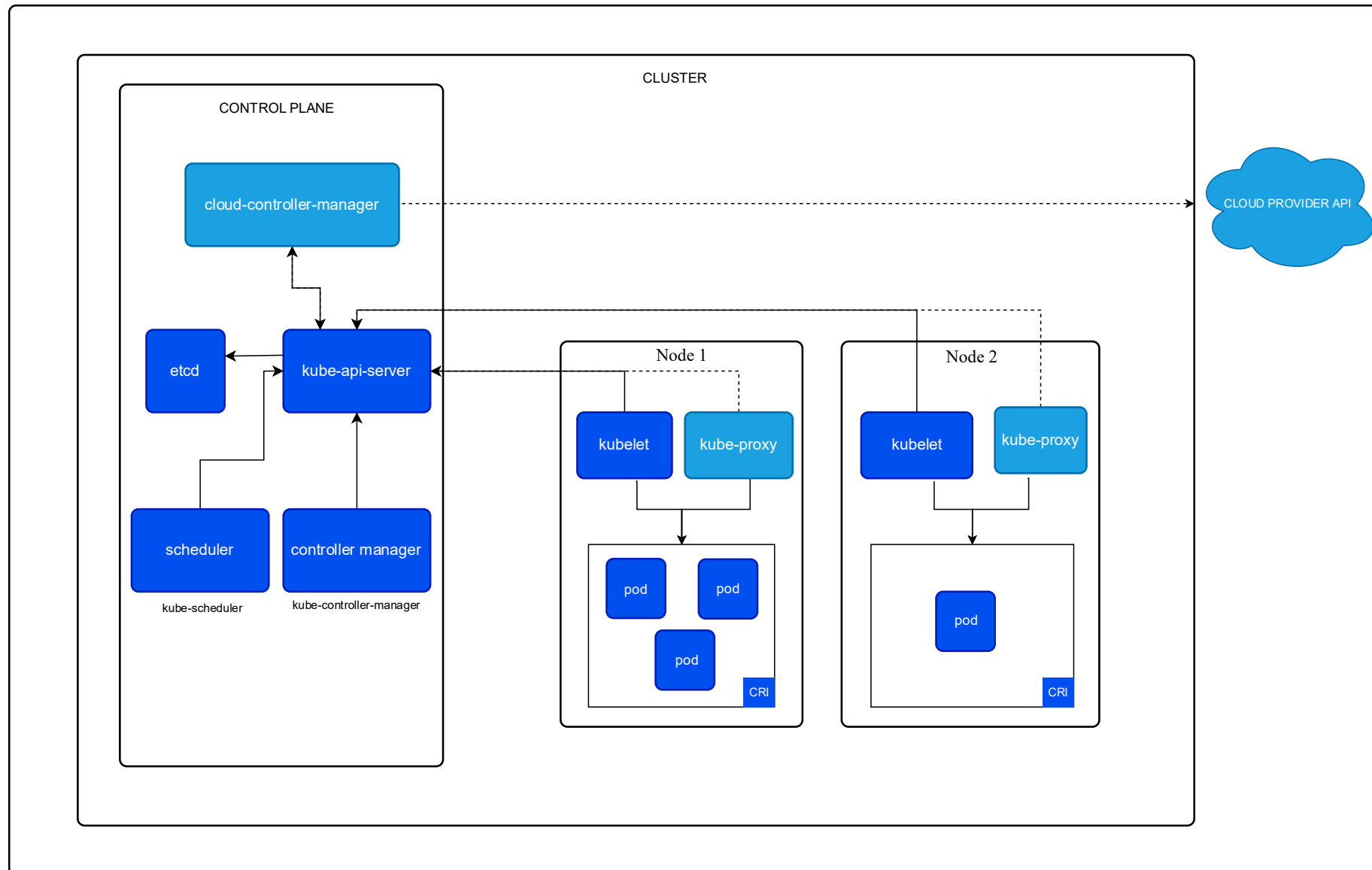
2. Tesla Kubernetes Breach

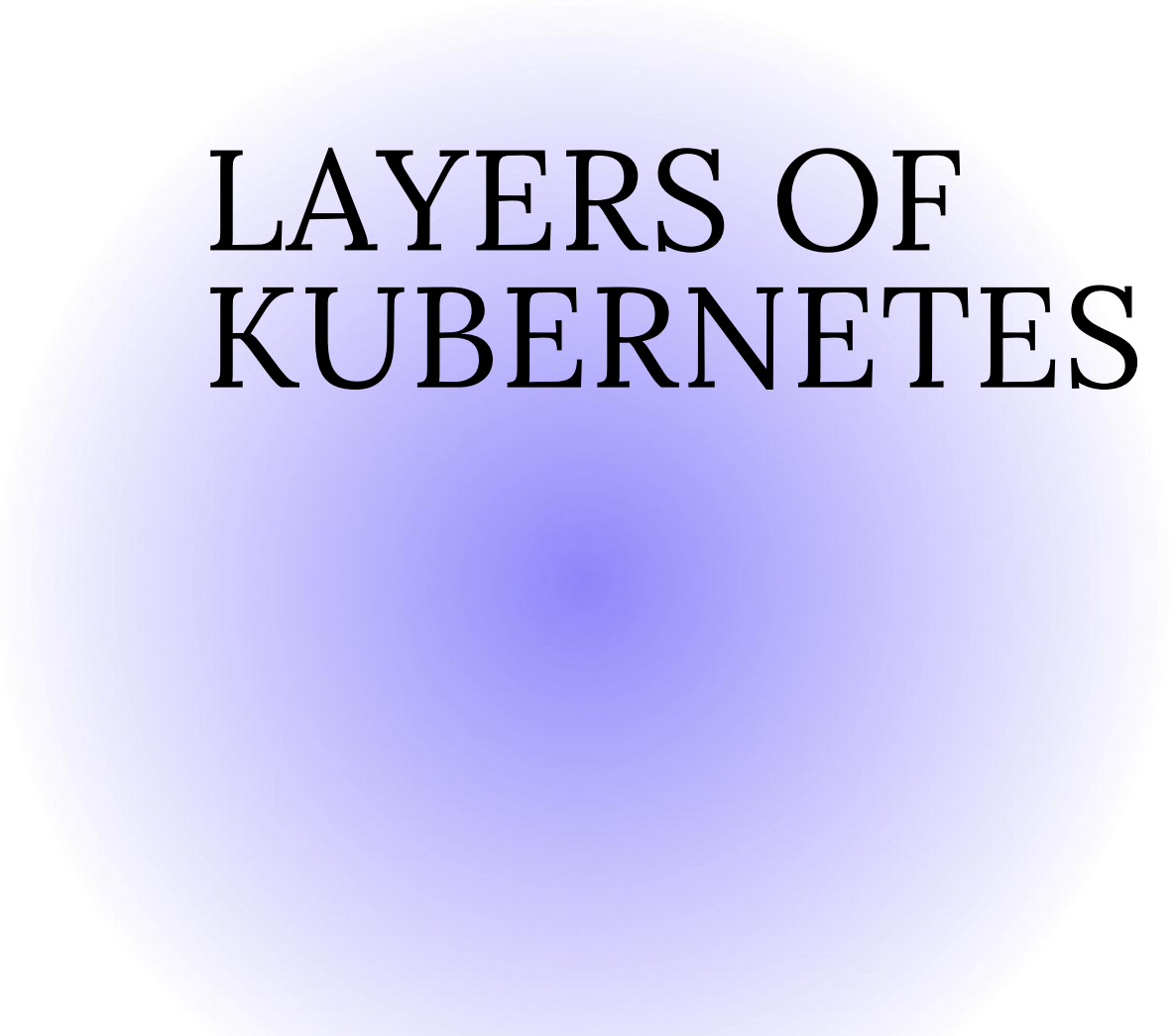
- Attackers leveraged cloud resources for cryptomining
- Exploited weak access controls and misconfigured workloads

3. “IngressNightmare” (Wiz Research)

- Critical Vulnerabilities in Ingress NGINX Controller
- Could allow remote code execution and cluster compromise

KUBERNETES ARCHITECTURE





LAYERS OF KUBERNETES SECURITY

LAYERS OF KUBERNETES SECURITY

1. Orchestration Layer Security
 2. Image Security
 3. CI/CD Pipeline Security
 4. Network Security
 5. Runtime Security
 6. Secrets Management
 7. Compliance & Auditing
- 

ORCHESTRATION LAYER SECURITY



✓ Core Components:

- OS, API server, etcd, scheduler, controller-manager

✓ Configuration Hardening

- Detect and remediate misconfigurations
- Use kube-bench (CIS Benchmark)

✓ Manage User & Permission – RBAC

- Apply the Principle of Least Privilege

CIS BENCHMARK

```
[INFO] 1 Master Node Security Configuration
[INFO] 1.1 API Server
[FAIL] 1.1.1 Ensure that the --allow-privileged argument is set to false (Scored)
[FAIL] 1.1.2 Ensure that the --anonymous-auth argument is set to false (Scored)
[PASS] 1.1.3 Ensure that the --basic-auth-file argument is not set (Scored)
[PASS] 1.1.4 Ensure that the --insecure-allow-any-token argument is not set (Scored)
[FAIL] 1.1.5 Ensure that the --kubelet-https argument is set to true (Scored)
[PASS] 1.1.6 Ensure that the --insecure-bind-address argument is not set (Scored)
[PASS] 1.1.7 Ensure that the --insecure-port argument is set to 0 (Scored)
[PASS] 1.1.8 Ensure that the --secure-port argument is not set to 0 (Scored)
[FAIL] 1.1.9 Ensure that the --profiling argument is set to false (Scored)
[FAIL] 1.1.10 Ensure that the --repair-malformed-updates argument is set to false (Scored)
[PASS] 1.1.11 Ensure that the admission control policy is not set to AlwaysAdmit (Scored)
[FAIL] 1.1.12 Ensure that the admission control policy is set to AlwaysPullImages (Scored)
[FAIL] 1.1.13 Ensure that the admission control policy is set to DenyEscalatingExec (Scored)
[FAIL] 1.1.14 Ensure that the admission control policy is set to SecurityContextDeny (Scored)
[PASS] 1.1.15 Ensure that the admission control policy is set to NamespaceLifecycle (Scored)
[FAIL] 1.1.16 Ensure that the --audit-log-path argument is set as appropriate (Scored)
[FAIL] 1.1.17 Ensure that the --audit-log-maxage argument is set to 30 or as appropriate (Scored)
[FAIL] 1.1.18 Ensure that the --audit-log-maxbackup argument is set to 10 or as appropriate (Scored)
[FAIL] 1.1.19 Ensure that the --audit-log-maxsize argument is set to 100 or as appropriate (Scored)
[PASS] 1.1.20 Ensure that the --authorization-mode argument is not set to AlwaysAllow (Scored)
[PASS] 1.1.21 Ensure that the --token-auth-file parameter is not set (Scored)
[FAIL] 1.1.22 Ensure that the --kubelet-certificate-authority argument is set as appropriate (Scored)
```

ORCHESTRATION LAYER SECURITY

✓ **Secure etcd**

- Enable TLS/mTLS for client-server communication
- Encrypt secrets at rest
- Restrict direct access

✓ **Configure security policies**

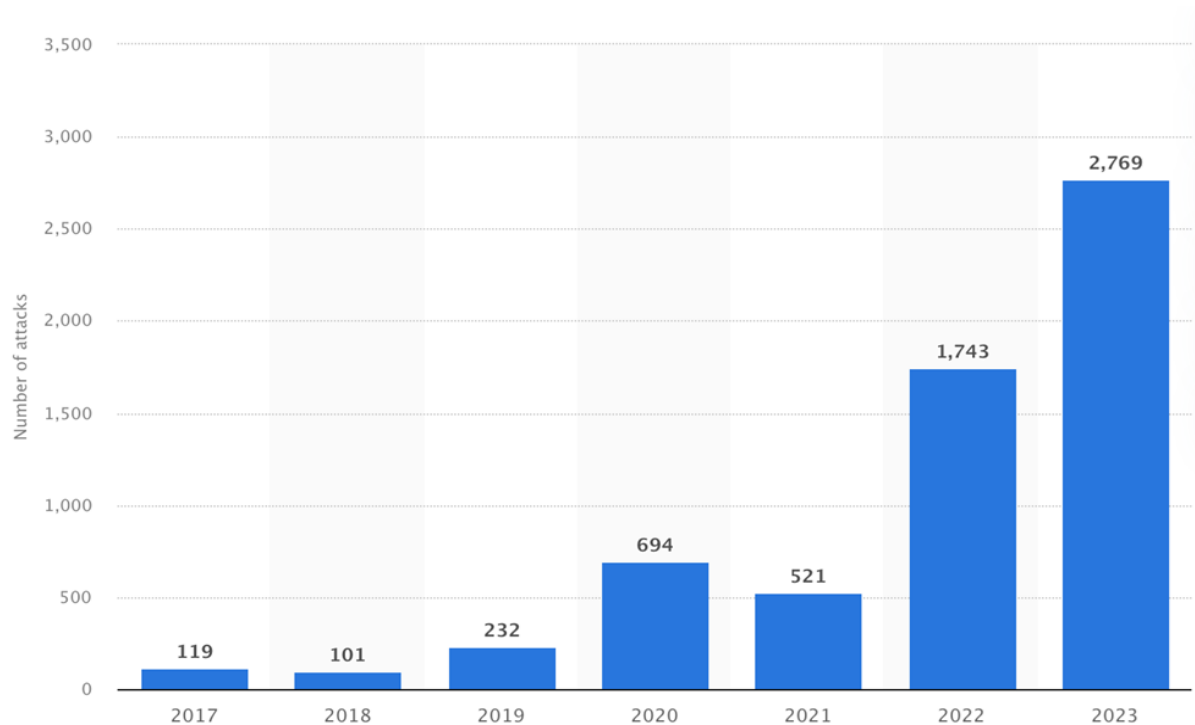
- Apply policy engines

✓ **Always Updated**

- Regularly update Kubernetes control plane & nodes



SUPPLY CHAIN ATTACK



ANNUAL NUMBER OF ENTITIES IMPACTED IN
SUPPLY CHAIN CYBER ATTACKS IN THE UNITED
STATES

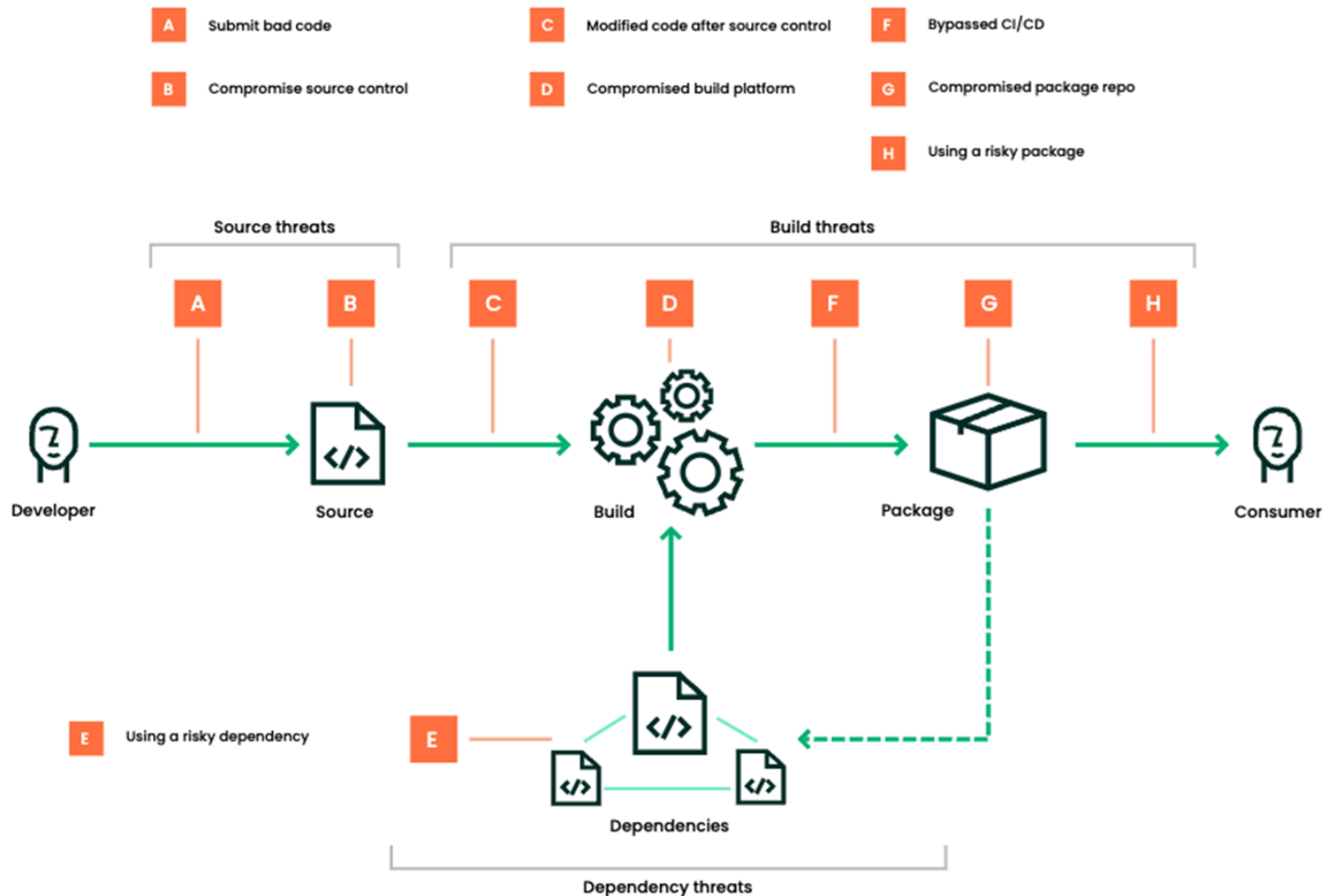
Recent major attacks

2024 – Linux xz backdoor vulnerabilities
(Source threats)

2022 – Log4j vulnerabilities
(Dependency threats)

2021 – Solarwinds
(Build threats)

SUPPLY CHAIN ATTACK



Source: <https://slsa.dev/images/supply-chain-threats.svg>

Source threats

Bad code that introduces vulnerabilities or a compromised source control system.

Build threats

Code commits to the build that were not tracked by the source control system, a compromised build platform, bypassing the CI/CD system, a compromised package repository, and injecting bad packages.

Dependency threats

Come into play where risky dependencies are used.

IMAGE SECURITY



- ✓ **Build Security Image**
 - Remove unnecessary packages, libraries
 - Avoid root user for running containers
- ✓ **Use trusted registries and base images**
- ✓ **Scan container images for vulnerabilities**

IMAGE SECURITY



Report Summary

Target	Type	Vulnerabilities	Secrets
python:3.4-alpine (alpine 3.9.2)	alpine	37	-
usr/local/lib/python3.4/site-packages/pip-19.0.3.dist-info/METADATA	python-pkg	3	-
usr/local/lib/python3.4/site-packages/setuptools-40.8.0.dist-info/METADATA	python-pkg	3	-
usr/local/lib/python3.4/site-packages/wheel-0.33.1.dist-info/METADATA	python-pkg	1	-

Legend:

- '-': Not scanned
- '0': Clean (no security findings detected)

python:3.4-alpine (alpine 3.9.2)

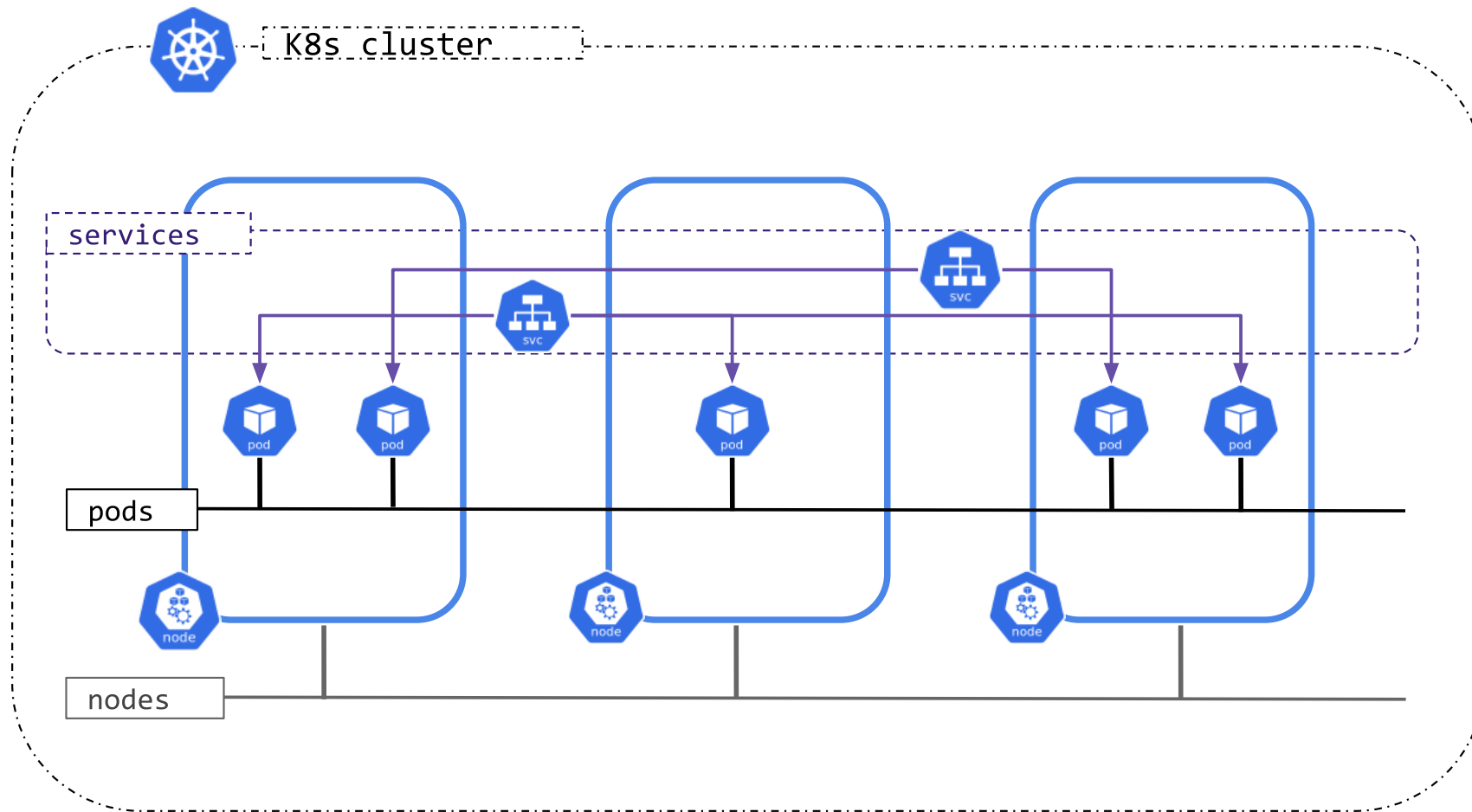
Total: 37 (UNKNOWN: 0, LOW: 4, MEDIUM: 16, HIGH: 13, CRITICAL: 4)

Library	Vulnerability	Severity	Status	Installed Version	Fixed Version	Title
expat	CVE-2018-20843	HIGH	fixed	2.2.6-r0	2.2.7-r0	expat: large number of colons in input makes parser consume high amount... https://avd.aquasec.com/nvd/cve-2018-20843
	CVE-2019-15903				2.2.7-r1	expat: heap-based buffer over-read via crafted XML input https://avd.aquasec.com/nvd/cve-2019-15903
libbz2	CVE-2019-12900	CRITICAL		1.0.6-r6	1.0.6-r7	bzip2: bzip2: Data integrity error when decompressing (with data integrity tests fail).... https://avd.aquasec.com/nvd/cve-2019-12900

CI/CD PIPELINE SECURITY

- ✓ **Scan code & dependencies**
 - Use SAST/DAST tools
- ✓ **Container image scanning**
- ✓ **Secure build pipelines**
 - Protect CI/CD servers
- ✓ **Enforce policy-as-code**
 - Integrate OPA/ Kyverno

NETWORK SECURITY



NETWORK SECURITY

- ✓ **Use Network Policies**

- Pod-to-pod communication controls

- ✓ **Service Mesh**

- Service-to-service traffic control
 - mTLS / encryption: secure connections between services.

- ✓ **Complementary Benefits**

- Zero Trust Networking
 - Observability



RUNTIME SECURITY

- ✓ **Monitor running containers**

- Observe container processes, network connections, file access, and resource usage.

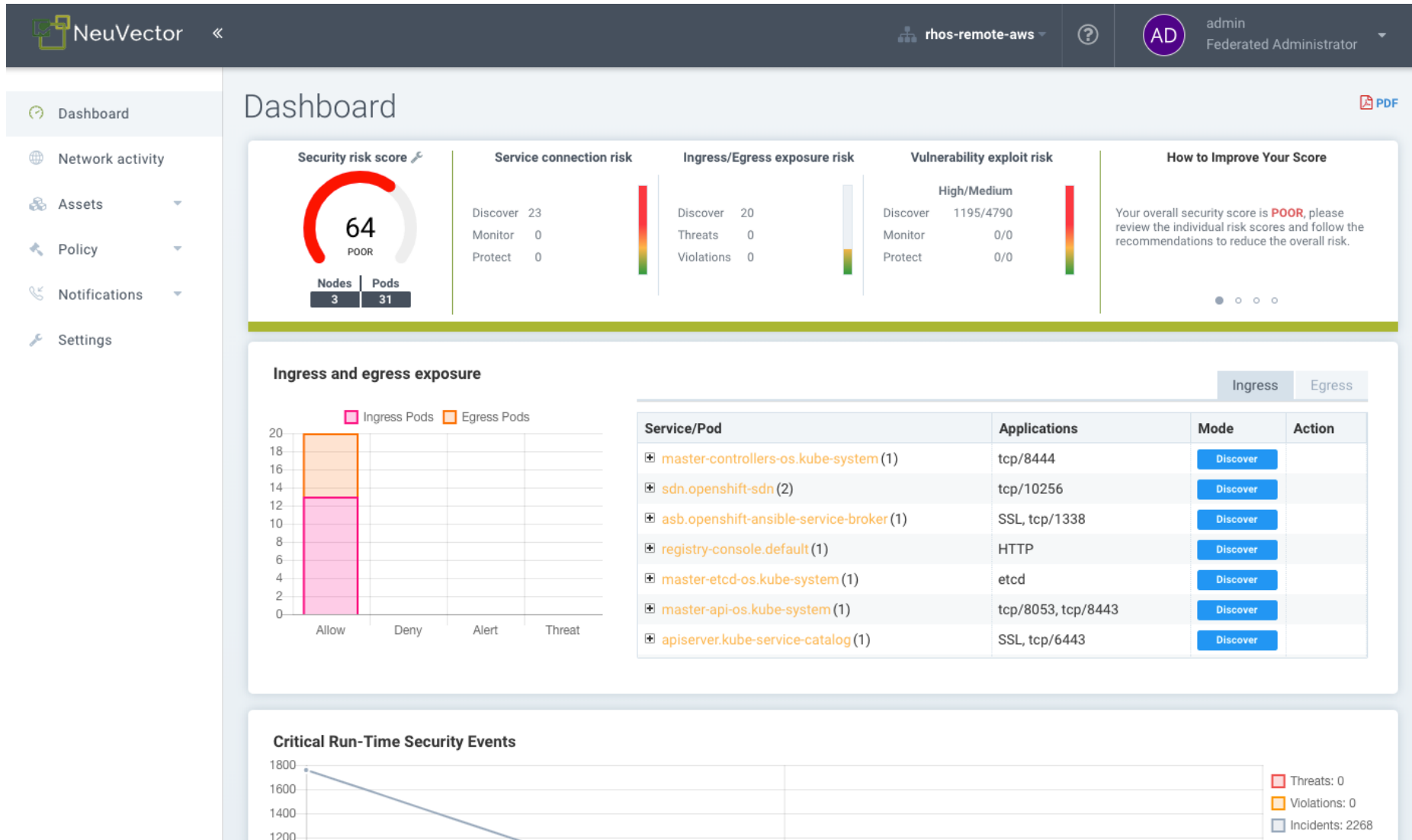
- ✓ **Detect anomalous behavior**

- Look for suspicious runtime activity: privilege escalation, unexpected network traffic, exec into pods.

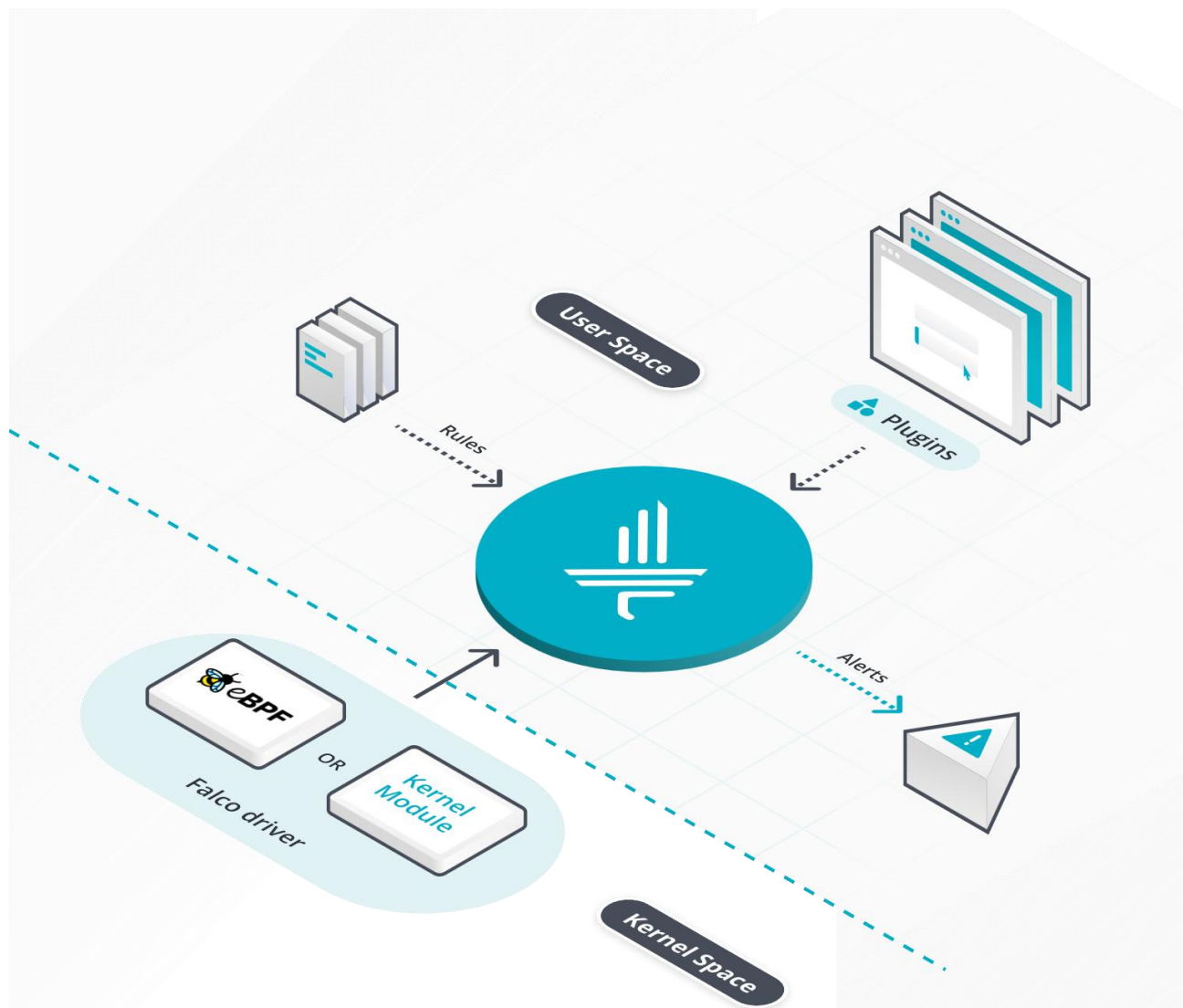
- ✓ **Apply Pod Security Standards**

- Enforce baseline/restricted policies on running pods.

RUNTIME SECURITY TOOLS



RUNTIME SECURITY TOOLS



SECRETS MANAGEMENT



- ✓ **Secure sensitive data**
 - passwords, tokens, API keys, certificates
- ✓ **Use external secret stores**
 - Hashi Corp Vault, AWS Secret Manager ...
- ✓ **Never hardcode secrets in CI/CD**
- ✓ **Avoid plain text in YAML**
 - Never write secrets directly in manifest files.

COMPLIANCE & AUDITING



- ✓ **Compliance Standards**
 - CIS Kubernetes benchmarks
 - PCI DSS, HIPAA, NIST
- ✓ **Enable Audit logging**
 - Track all API requests
- ✓ **Integrate SIEM system**
- ✓ **Continuous Auditing & Reporting**

BACKUP & DISASTER RECOVERY

1. Backup Critical Data

- etcd (cluster state, configs, secrets)
- Persistent Volumes (application data)
- Manifests, Helm charts, policies

2. Disaster Recovery Plan

- Define RPO (Recovery Point Objective) & RTO (Recovery Time Objective)
- Regularly test cluster restore procedures
- Keep offsite/remote copies of backups
- Automate failover and recovery workflows

USEFUL TOOLS

Security Layer	Recommended Tools	Purpose / Notes
Orchestration Layer	Kyverno, OPA, kube-bench	Policy-as-code, configuration compliance, CIS benchmark checks
Image Security	Trivy, Snyk	Scan container images for vulnerabilities and CVEs
CI/CD Pipeline Security	Snyk, Chekov	Scan code, dependencies, and pipeline configurations
Network Security	Cilium, Calico, Istio, Consul	Enforce network policies, service-to-service controls, mTLS
Runtime Security	NeuVector, kube-hunter, Falco	Monitor running containers, detect anomalies, enforce runtime policies
Secrets Management	HashiCorp Vault, AWS Secret Manager	Secure storage, encryption, dynamic secrets, access control
Compliance & Auditing	kube-bench, Kubescape	Continuous auditing, benchmark compliance, policy reporting

THANK YOU

Name: Shinebayar .Ts

Position: Senior cloud native architect, DLP LLC

Email: shinebayar.ts@dlp.mn

Q & A

