

ISOVALENT-ELITE

DURATION: 5 DAYS

PRICE: USD 4195

CLCs: 42

CE: 50

COURSE CODE: ISOVALENT-ELITE | **FORMAT:** Lecture & Lab

COURSE DESCRIPTION

Modern cloud-native environments demand a new approach to networking, security, and operations. As Kubernetes adoption continues to accelerate, engineers must understand how to design, deploy, secure, and operate dynamic application platforms that go far beyond traditional networking models — a shift where Cisco, through the Isovalent-built Cilium platform, now sits at the center.

ISOVALENT-ELITE is an official Cisco course, developed exclusively by Firefly, delivering comprehensive instructor-led training on the complete lifecycle of enterprise Cilium deployments — built on the eBPF-powered networking, security, and observability platform created by Isovalent, now part of Cisco. Across nine in-depth modules and extensive hands-on labs, students progress from Kubernetes networking fundamentals to advanced Cilium architecture, installation and deployment strategy, identity-based policy enforcement, service exposure and egress control, encryption and performance tuning, Hubble-driven observability, ClusterMesh

multi-cluster networking, and Tetragon-powered runtime security operations.

Designed around real-world enterprise scenarios, Isovalent-Elite focuses on the practical deployment strategies, operational best practices, and troubleshooting techniques that Cisco and Isovalent field teams rely on to confidently deploy and manage Cilium-powered Kubernetes environments across on-premises, hybrid, and multi-cloud infrastructures.

TARGET AUDIENCE

This course is designed for professionals responsible for designing, deploying, securing, and operating Kubernetes networking platforms, including:

- Network Engineers
- Cloud Infrastructure Engineers
- Platform Engineers
- Security Engineers
- Kubernetes Administrators

- DevOps Engineers
- Site Reliability Engineers (SRE)
- Solutions Architects
- Technical Consultants supporting cloud-native infrastructures

PREREQUISITES

Basic knowledge of Linux, Kubernetes, and container networking is recommended. Prior experience with Cilium is not required.

COURSE OBJECTIVES

Upon completion of this course, students will be able to:

- Understand cloud-native networking principles and Kubernetes networking architecture.
- Explain how eBPF enables high-performance networking, security, and observability within Kubernetes.
- Design and deploy Cilium as the primary networking platform for Kubernetes clusters.
- Select appropriate deployment models, routing strategies, and IP Address Management (IPAM) options.
- Implement identity-based security using Cilium Network Policies.
- Configure secure service exposure using Gateway API, LoadBalancer Services, and egress controls.
- Deploy and manage advanced networking features including routing, encryption, and high-performance datapaths.
- Design and operate multi-cluster Kubernetes environments using Cilium Cluster Mesh.
- Monitor, troubleshoot, and optimize Kubernetes networking using Hubble observability tools.

- Apply enterprise best practices for deployment, upgrades, validation, and day-to-day operations.

DETAILED COURSE STRUCTURE

Module 1 – Cloud Native Networking and Security

- Datacenter Foundations
- Traffic and Security Patterns
- Containers and Kubernetes Networking
- Cilium and eBPF
- Distribution and Production Planning

Module 2 – Kubernetes Fundamentals for Network and Security Teams

- Application Evolution and Container Foundations
- Kubernetes Control Plane and Core Objects
- Service Exposure, Configuration, and Storage Primitives
- Scheduling, Runtime Features, kube-proxy, and CNI Networking

Module 3 – ISOVALENT Introduction, Architecture, and Use Cases

- Enterprise Platform Context
- Cilium as a Platform Capability
- Enterprise Use Cases for Cilium
- Architecture, eBPF, and Datapath Mechanics

Module 4 – Installation Strategy and Deployment Workflow

- Deployment Strategy and Readiness
- Cilium Components and Node Integration
- Validation, Inspection, and Rollback
- IP Address Management Design
- CNI Lifecycle and Routing Modes

- Service Handling and kube-proxy Replacement
- Upgrades and Change Validation

Module 5 – External Communication, Service Exposure, and Egress Control

- External Communication Model and Packet Lifecycle
- Service Exposure and Gateway API
- External Reachability and Routing Integration
- Service Mesh and Cluster Mesh Context
- Egress Control and Policy-Driven Internet Access

Module 6 – ISOVALENT Policy Model and Security Architecture

- Why the Policy Model Matters
- Identity-Based Enforcement
- Policy Types and Structure
- Examples, Demos, and Policy Operations
- Hubble Policy Troubleshooting
- Policy Calculation and Datapath Internals
- Integrated Lab

Module 7 – Advanced Networking, Routing, Encryption, and Performance

- Transparent Encryption
- High-Performance Datapath and Load Balancing
- TLS and PKI Foundations
- Cilium Mutual Authentication and Gateway mTLS
- TLS Interception
- Demo and Integrated Lab

Module 8 – Multi-Cluster, Cloud and Observability

- Cluster Mesh and Multi-Cluster Fundamentals
- Global Services, Cross-Cluster Identity,

and Service Exposure

- Public Cloud and Hybrid Network Design
- Hubble Observability Architecture
- Hubble Operations, Metrics, and SIEM Integration
- Integrated Operations Checklist and Knowledge Review

Module 9 – Deep Security, Operations and Best Practices

- Runtime Security Foundations and eBPF
- TracingPolicy and Enforcement Model
- Tetragon Use Cases and Telemetry Integration
- RBAC and Access Governance
- Incident Response and Operational Troubleshooting
- Migration and Production Best Practices

Instructor Led Training

To view the schedule and secure your site

SIGN UP HERE