Zero Trust Security with SPIFFE and SPIRE (LFS482)

This course discusses the patterns and practices necessary for the adoption of Zero Trust Networking, as well as Zero Trust networking implementation models, use cases, scenarios, and outcomes enabled by open source software. You will install, make changes to, and operate SPIFFE and SPIRE deployments and harden your organization's security postures by operationalizing a "least privilege" authorization model.

Duration: 3 Days

Prerequisites for this course

Students should have practical experience with cloud computing platforms, deploying and managing Kubernetes clusters, and be familiar with Linux systems and command-line operations.

Outline for this course

Chapter 1 – Course Introduction

Chapter 2 - Foundations of Zero Trust

Chapter 3 - SPIFFE and SPIRE Concepts

Chapter 4 - Using SPIRE

Chapter 5 - Workload Identities

Chapter 6 - AuthZ and Policy Engines

Chapter 7 - SPIRE and AuthZ

Chapter 8 – SPIRE Architecture Considerations

Chapter 9 – SPIRE Day Two Ops

Chapter 10 - The SPIFFE Ecosystem