Detecting Cloud Runtime Threats with Falco (LFS254)

Learn about Falco and how to install and use it in securing cloud native environments.

Duration: 3 Days

Prerequisites for this course

- Basic concepts of cloud computing and cloud security.
- Basic concepts of cloud computing and cloud security.
- Basic understanding of system calls and their role in operating systems.
- Familiarity with Kubernetes, including concepts like Pods, Services, and Deployments.

Outline for this course

Chapter 1 – Course Introduction

Chapter 2 – Introduction to Falco

Chapter 3 – Getting Started with Falco

Chapter 4 – Syscall Data Source (Host Security)

Chapter 5 – Other Data Sources (Cloud Security)

Chapter 6 – Conditions and Fields

Chapter 7 – Falco Rules

Chapter 8 – Customizing Falco Rules

Chapter 9 – Outputs and Falcosidekick

Chapter 10 – Configuring Falco

Chapter 11 – Writing Falco Rules