Hewlett Packard
Enterprise

HPC – SECURITY DASHBOARD

VIT Vellore

CTY Members – Alok N, Arka Pramanik, Nishanth VM, Keshav Varshney, Swayam Atul Mehta

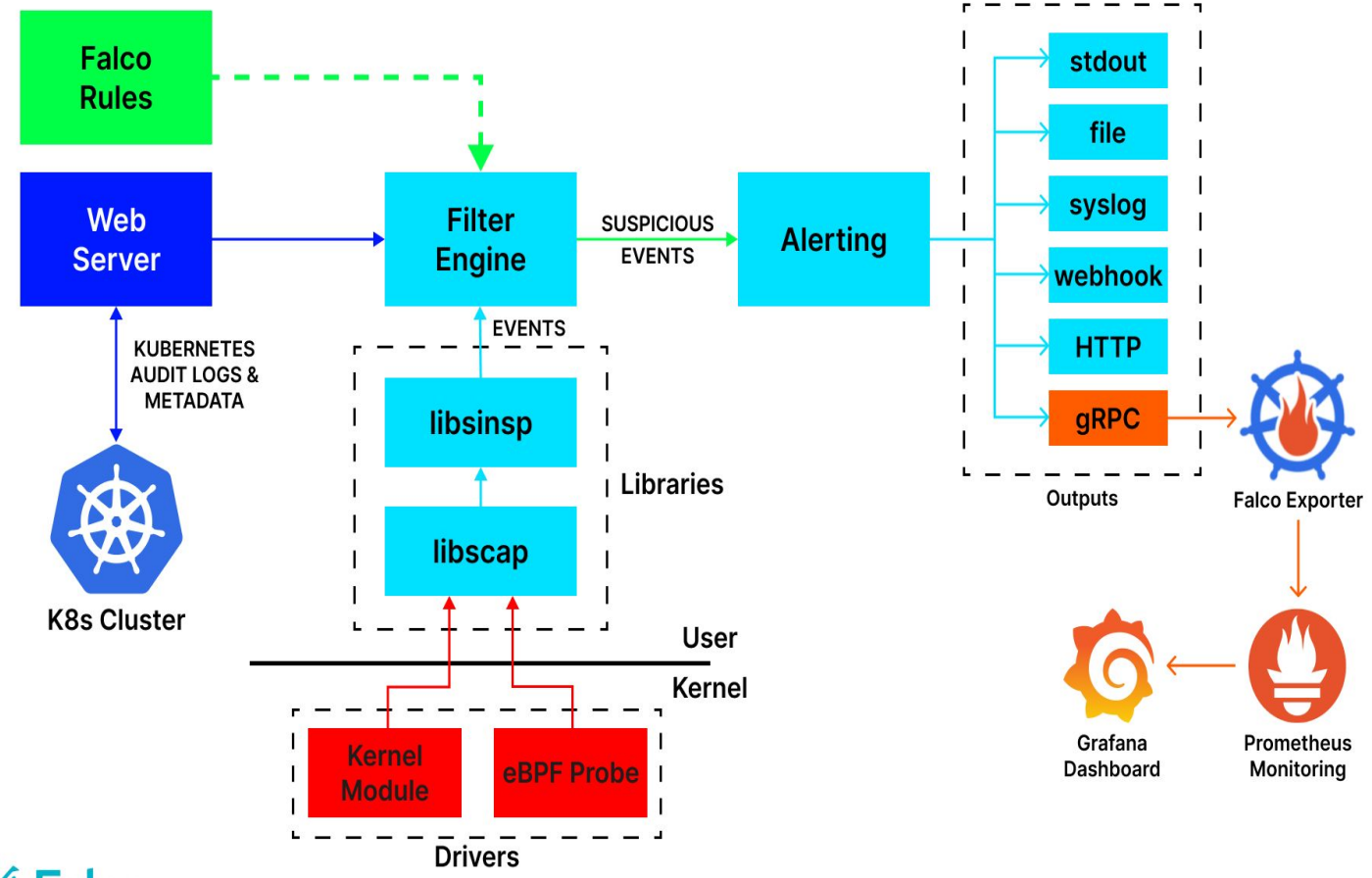
CTY Mentor – Yarlagadda Srinivasa Rao

VIT Mentor – Dr. Ruby D

31st May, 2023

PROJECT ARCHITECTURE, OBJECTIVES AND WORK-DONE

Architecture



Objectives

- Understand Kubernetes and runtime security.
- Secure a K8s cluster using Falco.
- Export Falco event metrics to Prometheus and Grafana.

Status

- Falco agents set up in K8s cluster.
- Suspicious events are sent as alerts.
- Grafana dashboard setup to visualize all Falco event metrics.

PROJECT PLAN , LEARNINGS , CHALLENGES

Learnings

- Kubernetes
- Docker
- Helm Charts
- Kubescape
- Prometheus monitoring and Grafana Dashboard
- eBPF technology and runtime security
- Falco architecture, rules, alerts and logs.

Challenges

- Resource constraints
- Building Falco probe driver for AKS nodes
- Falco issues with WSL 2.0

DEMO AND NEXT STEPS

Demo Objective

- Generate malicious system calls to trigger Falco.
- Visualize rate of Falco events using Grafana dashboard.
- Filter alerts based on various labels such as priority, tags, etc.

Next Steps

- Build on top of default ruleset to target specific actions.
- Prepare a standard remediation procedure for all kinds of malicious activities.
- Runtime security use cases.

Dashboard Screenshot

THANK YOU