TIGERA

Observability and Troubleshooting

Learn how to identify and resolve security gaps, performance and connectivity issues, and security policy violations

Summary:

The Calico Cloud Observability Clinic will build on your Kubernetes and containers skillset and help you complete your journey towards zero-trust workload security for your cloud-native applications. Tigera will review the fundamentals around security policy implementation,help identify security and audit gaps, provide guidance and recommendations to secure your cloud-native application using Dynamic Service and Threat Graph, Flow Visualizer, Policy Board and Command Line Interface. The clinic will enable you and your team to get an in-depth knowledge and steps and mechanism to use in order to assess your Kubernetes cluster's security posture, identify gaps in workload-workload communication and review security policies.

Scope

The Calico Cloud Observability Clinic covers the following,

- Overview of security policies and lab setup
- Investigation and troubleshooting using the UI and practice lab covering the Dynamic Service and Threat Graph, Flow Visualizer, Dynamic Packet Capture and Kibana
- Troubleshooting policy using the CLI and Dynamic Packet Capture with deep dive in policy rules implemented through IPTables and traffic flow logs followed by practical exercise to restore an application

Value

- Strengthen your understanding on the fundamentals of your Kubernetes cluster and containers Security Policies with Calico Cloud
- Gain in-depth knowledge on the workload-worklaod communication, upstream and downstream dependencies with Calico Cloud's Dynamic Service and Threat Graph, Flow Visualizer and custom dashboards.
- Learn, and practice, troubleshooting techniques with our hands-on labs
- Expand your knowledge on how Security Policies function at the dataplane
- Hands-on labs consisting of troubleshooting walkthroughs and "fix-it-yourself" scenarios

Delivery

1. Purchase Calico Observability Clinic

- Introductory session presenting the workshop and gathering specific requirements and area of interests

Observability and Troubleshooting

Learn how to identify and resolve security gaps, performance and connectivity issues, and security policy violations

2. Day 1

- Review fundamentals around workload communication, security policy deployment, configuration and best practices
- Walk through different troubleshooting scenarios by monitoring workload activity within the cluster
- Hands-on session starting with deployment of a test application, view workload-to-workload communication, security policies, workload access controls and troubleshooting

3. Day 2

- Review security policy implementation at the kernel and traffic flow log level
- Hands-on session to troubleshoot a security policy leveraging custom dashboards, Dynamic and Service Threat Graph and Flow Visualizer
- Hands-on session to troubleshoot a sample security policy at run time for an application with command line interface only

4. Deliverables

- Provide course documentation and recording for reference

TIGERA

Tigera, Inc.

58 Maiden Lane, Fl 5
San Francisco, CA 94108
+1 (415) 612-9546 / www.tigera.io

For more information, email us at contact@tigera.io.