Detection Strategies

Do not print this page. This is
property of the Securitydojo
Powered by Virtual Cybertron.

There are numerous methods for detecting incidents, each of these methods enables you to see your Kubernetes environment differently and aids in the early detection of potential problems, security risks, and system irregularities.

Logging and Monitoring

- This is the first and most basic level of detection. By collecting and analyzing logs and metrics from your Kubernetes cluster, you can identify trends and spot anomalies. Tools like Fluentd, Fluent Bit, Prometheus, Grafana, or the Elastic Stack (ELK Stack: Elasticsearch, Logstash, Kibana) can be used for this purpose.

Kubernetes Auditing

- Kubernetes Audit logs provide a record of the sequence of activities that have transpired in the cluster. It provides information like what happened, what resources were affected, and who initiated the action, etc. These logs can be used to detect anomalous behavior or unauthorized access.
- Understanding and Utilizing Audit Logs
    - By default, the audit logs feature is not enabled within the Kubernetes environment. By maintaining the record of all activities, audit logs can aid in identifying patterns & investigating incidents.
    - To successfully enable audit logs, there are a minimum of two prerequisites: the specification of a log path where the log files will be stored, and the creation of a policy file. The policy file defines what kinds of activities and resources should be logged.
    - These configurations must be set up within the kube-apiserver configuration, which is the core control component of Kubernetes. The kube-apiserver validates and configures data for api objects including pods, services, replicationcontrollers, and others.

Do not print this page. This is
property of the Securitydojo
Powered by Virtual Cybertron.

Kubernetes Events

- Kubernetes events are objects that provide insight into what is happening inside a cluster, such as decisions made by the scheduler or why some pods were evicted from the node. You can retrieve events through the kubectl describe command.

Network Policies

- Applying network policies and firewalls can help you control traffic to and from your applications within the cluster. Tools like Calico, Cilium, or kube-router can be used for managing network policies.

Security and Compliance Scanning Tools

- Tools like Aqua Security, Sysdig, or kube-bench can be used to scan your Kubernetes configuration files, Dockerfiles, or running resources for security risks, vulnerabilities, and non-compliance with best practices.

Threat Detection Solutions

- Falco is an example of a behavioral activity monitor designed to detect anomalous activity in your applications. Powered by Sysdig’s system call capture infrastructure, Falco lets you continuously monitor and detect container, application, host, and network activity.

Do not print this page. This is property of the Securitydojo Powered by Virtual Cybertron.