Delete Kubernetes events

A Kubernetes event is a Kubernetes object that logs state changes and failures of the resources in the cluster. Example events are a container creation, an image pull, or a pod scheduling on a node.

Info

ID: MS-TA9022
Tactic: Defense Evasion
MITRE technique: T1070

Kubernetes events can be very useful for identifying changes that occur in the cluster. Therefore, attackers may want to delete these events (e.g., by using: “kubectl delete events–all”) in an attempt to avoid detection of their activity in the cluster.

Mitigations

ID	Mitigation	Description
MS-M9020	Collect Logs to Remote Data Storage	Collect Kubernetes logs to a separate storage system.
MS-M9003	Adhere to least-privilege principle	Restrict permissions to delete Kubernetes events.