# Pod Modification, Data Component DC0030

Archived: 2026-04-05 17:00:26 UTC

Changes made to a pod's configuration or control data within a containerized cluster. This can include updating settings such as resource limits, environment variables, annotations, labels, or even the containers running within the pod. Pod modifications are often executed using commands like kubectl set, kubectl patch, or kubectl edit.

*Data Collection Measures:*

- Kubernetes API Server Audit Logs:
  - Capture all API calls related to pod modification, such as PATCH, PUT, or UPDATE methods on v1/pods.
- Runtime Security Tools:
  - Tools like Falco, Sysdig, and Kube-bench can monitor pod modifications at runtime and alert on policy violations.
- Container Orchestration Logs:
  - Monitor events logged by Kubernetes itself (e.g., `kubectl logs -n kube-system kube-controller-manager`).
- SIEM and EDR Solutions:
  - Use SIEM platforms (e.g., Splunk) to aggregate API server logs and detect patterns of unauthorized or suspicious pod modifications.
  - Endpoint Detection and Response (EDR) tools configured with container visibility can monitor commands like `kubectl` set or `kubectl patch`.
- Host-Based Monitoring:
  - Collect and analyze logs for processes executing `kubectl` commands or interacting with Kubernetes configuration files (e.g., `.kube/config`).

---

Source: https://attack.mitre.org/datacomponents/DC0030