Pod Enumeration, Data Component DC0037

Archived: 2026-04-02 10:43:12 UTC

Extracting a list of running or existing pods within a containerized cluster environment. Pods are the smallest deployable units in a Kubernetes cluster and typically represent an application or workload. Enumeration of pods provides insight into the structure and state of applications running in the cluster, such as the names of pods, their namespaces, and their associated metadata.

Data Collection Measures:

- Kubernetes API Server Audit Logs:
  - Enable Audit Logging in Kubernetes to capture API requests, such as GET `/api/v1/pods`.
- Container Runtime Logs:
  - Collect runtime-level logs from tools like CRI-O, containerd, or Docker, which might show relevant API calls for pod enumeration.
- EDR and SIEM:
  - Endpoint Detection and Response (EDR) tools, if configured with cluster-level visibility, can monitor user commands like `kubectl get pods`.
  - SIEM platforms (e.g., Splunk) can ingest Kubernetes API logs to detect enumeration patterns.
- Host-Based Monitoring:
  - Monitor processes and commands executed on nodes where `kubectl` is installed using tools like auditd, Sysmon for Linux, or kernel modules.

Source: https://attack.mitre.org/datacomponents/DC0037