Pod Creation, Data Component DC0019

Archived: 2026-04-05 18:30:36 UTC

The initial deployment or instantiation of a new pod in a containerized environment. This includes creating a pod manually, through orchestration tools (Kubernetes), or via Infrastructure-as-Code (IaC) configurations. A Pod is the smallest deployable unit in Kubernetes, typically containing one or more containers. Creation methods include:
- Direct pod deployment (`kubectl run` , `kubectl apply`)
- Automated deployment via CI/CD pipelines (e.g., ArgoCD, Jenkins, GitOps)
- Infrastructure-as-Code (IaC) templates (e.g., Terraform, Helm Charts)
- API-based deployments via Kubernetes control plane (create_pod API calls)
- Pods can be ephemeral (short-lived) or persistent (part of a StatefulSet or Deployment).

Data Collection Measures:

- Kubernetes Audit Logs
  - Captures all API requests, including pod `create` events.
- Kube-api server Logs
  - Monitors API calls related to pod deployments and modifications. Related Events: `PodSandboxChanged` , `SyncLoop` , `Created pod`
- Container Runtime Logs
  - Logs from CRI-O, containerd, or Docker capture pod creation events. Related Events: `container start` , `container create`
- Cloud Provider Logs
  - GKE, EKS, AKS logs provide insights into Kubernetes API interactions.
- SIEM & Log Aggregation
  - Integrates Kubernetes logs into SIEM solutions.
- EDR/XDR Solutions
  - Monitors container-based activity for anomalous pod creations.
