# Detection Strategy for Build Image on Host, Detection Strategy DET0459

Archived: 2026-04-05 14:55:10 UTC

**AN1261**

Detection of container image build activity directly on the host using Docker or Kubernetes APIs. Defenders may observe Docker build requests, anomalous Dockerfile instructions (such as downloading code from unknown IPs), or creation of new images followed by immediate deployment. This behavior chain typically consists of an unexpected image creation event correlated with outbound network communication to non-standard or untrusted destinations.

**Log Sources**

**Mutable Elements**

| Field | Description |
| --- | --- |
| RegistryAllowList | Defines trusted registries for image pulls/builds. Builds referencing unapproved registries may indicate adversary behavior. |
| NewImageThreshold | Threshold for number of new custom images created in a given time window. Exceeding this threshold may indicate malicious builds. |
| TimeWindow | Defines correlation window (e.g., 5m) between suspicious build activity and subsequent network traffic anomalies. |