# User Execution – Malicious Image (containers & IaaS) – pull/run → start → anomalous behavior (T1204.003), Detection Strategy DET0248

Archived: 2026-04-05 15:15:49 UTC

**AN0691**

CONTAINERS (Docker/K8s/containerd): A user pulls an untrusted image from a public/unknown registry and then creates/starts a container from that image. Shortly after start, the container spawns unexpected utilities (e.g., curl/wget/bash/python), or makes outbound network connections atypical for the namespace/workload. The analytic correlates Image Creation/Download → Container Creation → Container Start → Command Execution/Network activity within a short window and with a consistent image digest.

**Log Sources**

| Data Component | Name | Channel |
|---|---|---|
| Image Creation (DC0015) | containerd:events | Image pull from untrusted registry (name NOT IN allowlist) or new digest never seen before |
| Container Creation (DC0072) | kubernetes:audit | create: Pod/Container created with image tag 'latest' or mutable tag; imagePullPolicy=Always; noDigest=true |
| Container Start (DC0077) | kubernetes:events | start: ContainerStarted or Pulling image → Started container |
| Command Execution (DC0064) | auditd:SYSCALL | execve: Process in container namespace executes curl\|wget\|bash\|sh\|python\|nc with outbound args |
| Network Traffic Content (DC0085) | NSM:Flow | New egress from container IP/namespace to Internet or non-approved CIDRs/ASNs |

**Mutable Elements**

| Field | Description |
|---|---|
| ImageRegistryAllowList | Approved registries/namespaces (e.g., ECR/GCR/ACR org repos). |
| TimeWindow | Correlation window from image pull to container activity (e.g., ≤15m). |
| SuspiciousBinaries | Executables treated as high-risk when run in app containers (bash, sh, curl, wget, nc, powershell for Windows containers). |

| Field | Description |
| --- | --- |
| NamespaceScope | K8s namespaces that should never pull from Internet or run mutable tags. |
| OutboundCIDRBlockList | Destination networks/domains that should not be contacted by containers. |

### AN0692

IAAS (Cloud images/VMs): A new VM/instance is launched from a non-approved or newly-seen image (AMI/GCP Image/Azure Image). On first boot, cloud-init/user-data or embedded agents download code, spawn system utilities, or open outbound C2/mining traffic. The analytic correlates Instance/Image Creation → Instance Start → in-guest Process/Command Execution and/or anomalous network traffic.

#### Log Sources

#### Mutable Elements

| Field | Description |
| --- | --- |
| ApprovedImageCatalog | Set of golden images/owners and digest/IDs allowed to launch. |
| UserDataInspection | Whether to alert when userData/cloud-init contains exec or download directives. |
| FirstBootWindow | Time after start considered first-boot (e.g., ≤30m) for correlation. |
| VMTagScope | Restrict detection to prod or internet-facing subnets to reduce noise. |

---

Source: https://attack.mitre.org/detectionstrategies/DET0248#AN0692