Detection Strategy for Escape to Host, Detection Strategy DET0219

Archived: 2026-04-05 14:34:38 UTC

AN0612

Detection of container escape attempts via bind mounts, privileged containers, or abuse of docker.sock. Defenders may observe anomalous volume mount configurations (e.g., hostPath to / or /proc), unexpected privileged container launches, or use of container administration commands to access host resources. These events typically correlate with subsequent process execution on the host outside of normal container isolation.

Log Sources

Mutable Elements

Field	Description
AllowedHostPaths	List of directories permitted for hostPath volumes. Any access beyond these paths may be suspicious.
PrivilegedContainerThreshold	Number of privileged container launches expected in the environment. Exceeding this may indicate adversary behavior.

AN0613

Detection of Linux container escape attempts via syscalls (`unshare` , `keyctl` , `mount`) or process execution outside container namespaces. Defenders may correlate unusual system calls from containerized processes with subsequent process creation on the host or modification of host resources.

Log Sources

Data Component	Name	Channel
OS API Execution (DC0021)	auditd:SYSCALL	unshare, mount, keyctl, setns syscalls executed by containerized processes
Process Creation (DC0032)	linux:Sysmon	process creation events linked to container namespaces executing host-level binaries

Mutable Elements

Field	Description
SyscallWhitelist	Expected syscalls by containerized workloads. Deviations may signal an escape attempt.
TimeWindow	Defines correlation window (e.g., 60s) between suspicious syscalls and follow-on host process activity.

AN0614

Detection of Windows container escape attempts by observing processes accessing host directories, symbolic link abuse, or privilege escalation attempts. Defenders may detect anomalous process execution with access to system-level directories outside of container boundaries.

Log Sources

Mutable Elements

Field	Description
RestrictedHostDirs	Critical system paths containers should not access (e.g., C:\Windows, C:\ProgramData).

AN0615

Detection of ESXi escape attempts by monitoring for anomalies in hypervisor logs such as unexpected VM operations, privilege escalation events, or attempts to load malicious kernel modules within the hypervisor environment.

Log Sources

Data Component	Name	Channel
Kernel Module Load (DC0031)	esxi:vmkernel	VM exit/entry anomalies, unexpected hypercalls, or kernel module loading

Mutable Elements

Field	Description
AllowedKernelModules	Modules permitted in the hypervisor. Loading any module outside of this list may indicate compromise.
