Detection Strategy for ESXi Administration Command, Detection Strategy DET0232

Archived: 2026-04-05 12:57:40 UTC

AN0646

Detects anomalous usage of ESXi Guest Operations APIs such as StartProgramInGuest, ListProcessesInGuest, ListFileInGuest, or InitiateFileTransferFromGuest. Defender perspective focuses on unusual frequency of guest API calls, invocation from unexpected management accounts, or execution outside of business hours. These correlated signals indicate adversarial abuse of ESXi administrative services to run commands on guest VMs.

Log Sources

Data Component	Name	Channel
Application Log Content (DC0038)	esxi:hostd	Guest Operations API invocation: StartProgramInGuest, ListProcessesInGuest, ListFileInGuest, InitiateFileTransferFromGuest

Mutable Elements

Field	Description
ExpectedAdminUsers	Whitelist of management accounts authorized to use ESXi Guest Ops APIs.
TimeWindow	Business hours during which Guest Ops API usage is expected; activity outside may be suspicious.
OperationThreshold	Number of Guest Ops API calls considered anomalous if exceeded in a given timeframe.
AuthorizedVMs	List of VMs where Guest Ops usage is permitted; usage on other VMs may indicate malicious activity.
