Detection of Unix Shell, Detection Strategy DET0607

Archived: 2026-04-05 17:19:00 UTC

AN1657

Command-line activities can potentially be detected through Mobile Threat Defense (MTD) integrations with lower-level OS APIs. This could grant the MTD agents access to running processes and their parameters, potentially detecting unwanted or malicious shells.
Mobile Threat Defense (MTD) with lower-level OS APIs integrations may have access to newly created processes and their parameters, potentially detecting unwanted or malicious shells.
Application vetting services could detect the invocations of methods that could be used to execute shell commands.[1]
Mobile Threat Defense (MTD) with lower-level OS APIs integrations may have access to running processes and their parameters, potentially detecting unwanted or malicious shells.

Log Sources

AN1658

Command-line activities can potentially be detected through Mobile Threat Defense (MTD) integrations with lower-level OS APIs. This could grant the MTD agents access to running processes and their parameters, potentially detecting unwanted or malicious shells.
Mobile Threat Defense (MTD) with lower-level OS APIs integrations may have access to newly created processes and their parameters, potentially detecting unwanted or malicious shells.
Application vetting services could detect the invocations of methods that could be used to execute shell commands.[1]
Mobile Threat Defense (MTD) with lower-level OS APIs integrations may have access to running processes and their parameters, potentially detecting unwanted or malicious shells.

Log Sources
