Behavioral Detection of Unix Shell Execution, Detection Strategy DET0384

Archived: 2026-04-05 14:54:29 UTC

AN1081

Detects bash, sh, zsh, or BusyBox shell execution initiated via remote sessions, unauthorized users, or embedded within secondary script interpreters. Focus is on chained behavior: shell > suspicious commands > network discovery or persistence indicators.

Log Sources

Mutable Elements

Field	Description
ExecutableName	Detect variants like /bin/sh, /usr/local/bin/zsh, /bin/busybox sh.
UserContext	Shell used by service accounts, root, or rare accounts.
ParentProcess	Shell invoked by unexpected parents (e.g., curl, mail, apache2).
TimeWindow	Execution outside maintenance windows or normal activity periods.
CommandLinePattern	Flags use of loops, download commands, chaining (|, &&), or reverse shells.

AN1082

Identifies use of sh/bash/zsh in suspicious context, such as user scripts launched from non-standard apps (e.g., Preview.app), embedded in LaunchDaemons, or executed outside Terminal.app. Looks for misuse in Automator, LaunchAgents, or NSAppleScript-executed shell.

Log Sources

Mutable Elements

Field	Description
ScriptLocation	Execution from /Users/Shared, ~/Library/LaunchAgents, /tmp.
ParentProcess	Shells spawned from Preview, Safari, or AppleScript.
UserRole	Detection thresholds may differ for admin vs standard users.

AN1083

Detects BusyBox or Ash shell execution from unauthorized logins or remote connections. Focus is on rare shell invocations from DCUI, SSH sessions, or remote management paths. Also watches for payload droppers or persistence artifacts using shell.

Log Sources

Mutable Elements

Field	Description
UserContext	Non-root use of shell (or root outside maintenance window).
CommandPattern	Use of ‘nc’, ‘wget’, or dropper-like behavior in shell.
ShellPath	Unexpected invocation of BusyBox/ash from mounted ISO or datastore.

AN1084

Detects Unix shell usage on network appliances (e.g., routers, firewalls, embedded Linux) through rare console commands, CLI interfaces, or script injection via exposed APIs or SSH.

Log Sources

Mutable Elements

Field	Description
Interface	Flags command line access via remote console (telnet/SSH/API) from non-whitelisted source.
CommandString	Monitors rare/privileged shell commands (e.g., enable, tftp, firmware mod).
