Detection for Spoofing Security Alerting across OS Platforms, Detection Strategy DET0311

Archived: 2026-04-02 11:11:50 UTC

AN0868

Detection of inconsistencies between reported sensor health and actual process/service state. For example, Windows Defender tray icon/UI showing healthy status while corresponding Defender services (WinDefend, MsMpEng) are stopped or disabled. Correlates process creation events with missing or terminated security processes and spoofed health events.

Log Sources

Mutable Elements

Field	Description
ServiceNameList	Monitored list of critical security service names; environment-specific.
FakeUIProcessPatterns	Patterns of filenames or paths mimicking Windows Security GUI elements.

AN0869

Monitoring for discrepancies between system daemon/service state and reported health messages (e.g., syslog shows AV/IDS daemon stopped, but spoofed messages claim it is still running). Detects userland processes impersonating AV/IDS command-line outputs or modifying log forwarding configurations.

Log Sources

Data Component	Name	Channel
Process Creation (DC0032)	auditd:SYSCALL	execve: Execution of binaries/scripts presenting false health messages for security daemons
Host Status (DC0018)	linux:syslog	Service stop or disable messages for security tools not reflected in SIEM alerts

Mutable Elements

Field	Description
SecurityDaemonList	Names of AV/IDS/EDR daemons monitored in Linux environments.

AN0870

Detection of fake or spoofed macOS Security & Privacy GUIs showing healthy status after XProtect, Gatekeeper, or AV processes are disabled. Correlates user-space UI process creation with terminated or missing security daemons.

Log Sources

Data Component	Name	Channel
Process Creation (DC0032)	macos:unifiedlog	Execution of processes mimicking Apple Security & Privacy GUIs
Host Status (DC0018)	macos:unifiedlog	Termination or disabling of XProtect, Gatekeeper, or third-party AV daemons

Mutable Elements

Field	Description
TrustedDaemonList	Monitored list of macOS security daemons such as XProtect, Gatekeeper, or third-party AV.
