Detection Strategy for Event Triggered Execution via emond on macOS, Detection Strategy DET0555

Archived: 2026-04-05 15:50:13 UTC

AN1534

Detection focuses on identifying unauthorized file creation or modification within `/etc/emond.d/rules/` or `/private/var/db/emondClients`, which indicate attempts to register a malicious emond rule. Correlate with process execution of `/sbin/emond` and any launched commands it invokes, especially during boot or login events. Anomalies may include rules created by non-root users or unexpected shell commands executed by emond.

Log Sources

Mutable Elements

Field	Description
PathPrefix	Paths such as `/etc/emond.d/rules/` and `/private/var/db/emondClients` may vary slightly or be symlinked in some setups
TimeWindow	The time range for correlating rule file creation to emond execution may be tuned based on system performance and usage
ParentProcessFilter	Defenders may wish to restrict alerts to emond processes not spawned from trusted system update or provisioning tools
CommandPatternList	List of known suspicious commands or binaries used by adversaries (e.g., reverse shells, persistence scripts)
