Detection of Systemd Service Creation or Modification on Linux, Detection Strategy DET0253

Archived: 2026-04-05 16:24:42 UTC

AN0701

Detects the creation or modification of `.service` unit files in system/user-level directories, combined with execution of `systemctl`, `service`, or dynamically created drop-ins via systemd generators. Detects persistence by analyzing the `ExecStart` path, file entropy, and symlink usage, especially when paired with execution from `/tmp`, `/dev/shm`, or unmounted volumes.

Log Sources

Mutable Elements

Field	Description
ServicePathRegex	Regex filters for systemd unit locations (e.g., `/etc/systemd/system/*.service`, `/lib/systemd/system/`)
ExecStartPathAllowlist	Allowlist of trusted `ExecStart` binary paths (e.g., `/usr/bin/`, `/bin/`)
UserContextFilter	List of usernames that are authorized to define user-level services
FileEntropyThreshold	Entropy level of binaries referenced in `ExecStart` to detect packed or obfuscated payloads
SystemctlOperationSet	Flags suspicious combinations such as `systemctl enable` + `systemctl start` within short interval

---