Detection Strategy for Kernel Modules and Extensions Autostart Execution, Detection Strategy DET0450

Archived: 2026-04-05 13:02:00 UTC

AN1243

Monitor kernel module load/unload activity via modprobe, insmod, rmmod, or direct manipulation of /lib/modules. Correlate with installation of kernel headers, compilation commands, or downloads of .ko files. Detect anomalies in unsigned module loading or repeated module load attempts under non-root users.

Log Sources

Data Component	Name	Channel
Command Execution (DC0064)	auditd:SYSCALL	Execution of insmod, modprobe, or rmmod commands by non-standard users or outside expected timeframes
File Creation (DC0039)	auditd:SYSCALL	Access or modification to /lib/modules or creation of .ko files
File Modification (DC0061)	linux:osquery	New or modified kernel object files (.ko) within /lib/modules directory

Mutable Elements

Field	Description
UserContext	Scope detection to non-root or unexpected users performing module-related activity
TimeWindow	Limit alerts to module activity outside approved change windows
FilePathRegex	Adjust regex pattern for directories to monitor depending on kernel version or distro

AN1244

Detect user-initiated kextload commands or modifications to /Library/Extensions. Correlate with changes to KextPolicy database or unauthorized developer signing identities. Alert on attempts to disable SIP or load legacy extensions from unsigned sources.

Log Sources

Mutable Elements

Field	Description
DeveloperIDAllowlist	Approved developer IDs whose kexts should not trigger alerts
KextLoadTimeWindow	Threshold for detecting kext loads outside standard install/update operations
SignatureCheckFlag	Flag to enforce strict signing checks depending on SIP status

---