Detect Suspicious Access to securityd Memory for Credential Extraction, Detection Strategy DET0057

Archived: 2026-04-02 12:44:05 UTC

AN0156

Detects suspicious memory access attempts targeting the `securityd` process. Observes tools invoking process memory read operations (e.g., ptrace, task_for_pid) against `securityd`. Correlates with anomalous parent process lineage, root privilege escalation, or repeated unauthorized attempts.

Log Sources

Mutable Elements

Field	Description
AllowedDebuggers	List of authorized debugging tools permitted in dev/test environments
TimeWindow	Correlation period between memory inspection and Keychain API access
PrivilegedUsers	Expected set of admin accounts with legitimate debugging permissions

AN0157

Detects adversaries attempting to attach debuggers or memory dump utilities to credential storage daemons analogous to macOS `securityd`. Observes ptrace syscalls, /proc//mem access, or gcore dumps against sensitive processes. Correlates anomalies with privilege escalation or credential dumping attempts.

Log Sources

Mutable Elements

Field	Description
MonitoredProcesses	List of credential storage daemons (e.g., securityd, gnome-keyring, kwallet) monitored for memory access attempts
CorrelationDepth	Defines how many chained events (process execution + syscall + file read) to correlate before raising an alert
PrivilegeContext	Expected user/group context for processes allowed to access protected memory

Source: https://attack.mitre.org/detectionstrategies/DET0057#AN0157