Detect Access or Search for Unsecured Credentials Across Platforms, Detection Strategy DET0412

Archived: 2026-04-05 17:01:08 UTC

AN1153

Unusual access to bash history, registry credentials paths, or private key files by unauthorized or scripting tools, with correlated file and process activity.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Defines the threshold time for accessing multiple sensitive files indicating automation.
SuspiciousProcessList	Process names to monitor (e.g., reg.exe, cmd.exe, powershell.exe, etc.)

AN1154

Reading of sensitive files like .bash_history, /etc/shadow, or private key directories by unauthorized users or unusual processes.

Log Sources

Mutable Elements

Field	Description
SensitivePaths	Paths to credential files such as /etc/shadow or ~/.bash_history
UserContext	Whether the process runs under a privileged or non-interactive session

AN1155

Unusual access to ~/Library/Keychains, ~/.bash_history, or Terminal command history by unauthorized processes or users.

Log Sources

Data Component	Name	Channel
File Access (DC0055)	macos:unifiedlog	read access to ~/Library/Keychains or history files by terminal processes
Command Execution (DC0064)	macos:unifiedlog	execution of 'security', 'cat', or 'grep' commands accessing credential storage

Mutable Elements

Field	Description
ProcessName	Tool or command used to query credentials (e.g., security, grep)
TargetPath	Credential file paths (e.g., ~/Library/Keychains)

AN1156

Unusual web-based access or API scraping of password managers, single sign-on sessions, or credential sync services via browser automation or anomalous API tokens.

Log Sources

Mutable Elements

Field	Description
TokenAnomalyThreshold	Scoring threshold for access token entropy, reuse, or bot-like patterns
AccessGeoLocation	Region anomalies in SaaS portal access

AN1157

Unauthorized API or console calls to retrieve or reset password credentials, download key material, or modify SSO settings.

Log Sources

Mutable Elements

Field	Description
SSOSettingScope	Subset of IdP settings monitored for unauthorized changes
SecretType	Which secrets (passwords, keys, tokens) are monitored

AN1158

Access to container image layers or mounted secrets (e.g., Docker secrets) by processes not tied to entrypoint or orchestration context.

Log Sources

Data Component	Name	Channel
File Access (DC0055)	auditd:SYSCALL	read of /run/secrets or docker volumes by non-entrypoint process
Process Creation (DC0032)	containerd:Events	unusual process spawned from container image context

Mutable Elements

Field	Description
EntrypointAllowlist	Container entrypoints that are permitted to read secrets
VolumeMountPath	Paths to credentials/secrets inside container images

AN1159

Use of configuration backup utilities or CLI access to dump plaintext passwords, local user hashes, or SNMP strings.

Log Sources

Mutable Elements

Field	Description
ManagementInterfaceIPs	IP ranges authorized to perform credential dumps
CommandPattern	Regex patterns for suspicious CLI commands
