

# Detect Credentials Access from Password Stores, Detection Strategy DET0430

Archived: 2026-04-05 13:42:22 UTC

## AN1198

Monitors suspicious access to password stores such as LSASS, DPAPI, Windows Credential Manager, or browser credential databases. Detects anomalous process-to-process access (e.g., Mimikatz accessing LSASS) and correlation of credential store file reads with execution of non-standard processes.

### Log Sources

### Mutable Elements

Field	Description
TargetProcesses	List of sensitive processes to monitor (e.g., lsass.exe, svchost.exe)
KeywordPatterns	Regex for suspicious command-line arguments such as 'dpapi', 'credman', 'mimikatz'

## AN1199

Detects access to known password store files (e.g., /etc/shadow, GNOME Keyring, KWallet, browser credential databases). Monitors anomalous process read attempts and suspicious API calls that attempt to extract stored credentials.

### Log Sources

### Mutable Elements

Field	Description
MonitoredFiles	Paths to password storage files (e.g., /etc/shadow, ~/.local/share/keyrings/)
SuspiciousCommands	Process or command-line keywords that indicate password extraction attempts

## AN1200

Monitors Keychain database access and suspicious invocations of security and osascript utilities. Correlates process execution with attempts to dump or unlock Keychain data.

### Log Sources

**Mutable Elements**

<b>Field</b>	<b>Description</b>
AllowedApplications	Whitelist of legitimate processes accessing the Keychain
AlertThreshold	Number of failed access attempts before raising an alert

**AN1201**

Detects attempts to access or enumerate cloud password/secrets storage services such as AWS Secrets Manager, Azure Key Vault, or GCP Secret Manager. Monitors API calls for abnormal enumeration or bulk retrieval of secrets.

**Log Sources**

**Mutable Elements**

<b>Field</b>	<b>Description</b>
UserContext	Correlate cloud API calls with IAM role, user, or service account context
AccessThreshold	Number of secret retrievals within a time window before flagging

---

Source: <https://attack.mitre.org/detectionstrategies/DET0430#AN1199>