Detect Modification of Authentication Processes Across Platforms, Detection Strategy DET0104

Archived: 2026-04-02 11:29:26 UTC

AN0287

Detects modification of LSASS and authentication DLLs, suspicious registry changes to password filter packages, and abnormal process access to lsass.exe. Correlates registry modifications, DLL loads, and process handle access events.

Log Sources

Mutable Elements

Field	Description
MonitoredRegistryKeys	Specific LSASS and password filter registry paths monitored for modification.
TimeWindow	Correlation window between registry change, DLL load, and lsass.exe access.

AN0288

Detects modification of PAM configuration files, unauthorized new PAM modules, and suspicious process execution accessing PAM-related binaries. Correlates file modification events in /etc/pam.d/ with process execution of unauthorized binaries.

Log Sources

Mutable Elements

Field	Description
WatchedPaths	Critical PAM directories and configuration files monitored for modification.

AN0289

Detects unauthorized additions or changes to /Library/Security/SecurityAgentPlugins and suspicious process activity attempting to hook authentication APIs. Correlates file modifications with abnormal plugin loads in authentication flows.

Log Sources

Mutable Elements

Field	Description
PluginPaths	List of approved authentication plugin directories to baseline.

AN0290

Detects suspicious configuration changes in IdP authentication flows such as enabling reversible password encryption, MFA bypass, or policy weakening. Correlates policy modification events with unusual administrative activity.

Log Sources

Mutable Elements

Field	Description
PolicyBaseline	Expected authentication-related policy configurations to compare against.

AN0291

Detects unauthorized changes to IAM authentication configurations such as disabling MFA, creating backdoor access keys, or altering trust policies. Correlates identity policy updates with unusual login behavior.

Log Sources

Mutable Elements

Field	Description
ApprovedAccounts	Baseline list of service accounts expected to modify IAM authentication policies.

Source: https://attack.mitre.org/detectionstrategies/DET0104#AN0290