Detect Hybrid Identity Authentication Process Modification, Detection Strategy DET0293

Archived: 2026-04-05 13:02:15 UTC

AN0814

Detects injection or tampering of DLLs in hybrid identity agents (e.g., AzureADConnectAuthenticationAgentService), registry or configuration changes tied to PTA/AD FS, and anomalous LSASS or AD FS module loads correlated with authentication anomalies.

Log Sources

Mutable Elements

Field	Description
WatchedServices	Hybrid identity services monitored for tampering, e.g., PTA agent, AD FS.
TimeWindow	Window correlating DLL/module load events with logon anomalies.

AN0815

Detects registration of new PTA agents, conditional access changes disabling hybrid MFA enforcement, or suspicious updates to AD FS token-signing configurations.

Log Sources

Mutable Elements

Field	Description
PrivilegedRoles	Roles authorized to configure PTA/AD FS integrations.

AN0816

Detects API calls registering or updating hybrid identity connectors, modification of cloud-to-on-premises federation trust, and unusual token issuance logs.

Log Sources

Mutable Elements

Field	Description
MonitoredFederations	Federation trusts and connectors relevant to hybrid identity setup.

AN0817

Detects tenant-wide authentication or conditional access changes that weaken hybrid identity enforcement, including disabling AD FS or bypassing hybrid MFA policies.

Log Sources

Mutable Elements

Field	Description
PolicyScope	Scope of authentication and federation policies to be monitored.

AN0818

Detects suspicious changes to SAML/OAuth federation configurations, such as new signing certificates, altered endpoints, or claims issuance rules granting elevated privileges.

Log Sources

Mutable Elements

Field	Description
FederationEndpoints	Federation/SAML endpoints monitored for modification.
