Behavioral Detection Strategy for Use Alternate Authentication Material (T1550), Detection Strategy DET0338

Archived: 2026-04-05 16:11:55 UTC

AN0954

Use of stolen Kerberos tickets or token impersonation resulting in logon sessions from accounts without expected interactive logon events.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Allows tuning of how far apart related logon and process events can be correlated
UserContext	Customize for high-value or service accounts with restricted access policies

AN0955

Access tokens or SSH keys used without corresponding login shell or PAM module activity, particularly for remote execution.

Log Sources

Mutable Elements

Field	Description
SourceIPWhitelist	Tune for approved jump boxes or bastion hosts
AuthMethod	Filter on use of password vs publickey methods for better coverage

AN0956

Token replay or impersonation in federated logins without interactive browser session or MFA prompts.

Log Sources

Mutable Elements

Field	Description
MFAContextRequired	Customize for accounts where MFA must always precede token issuance
RefreshTokenReuseThreshold	Threshold for number of times a refresh token is reused without re-auth

AN0957

Unusual reuse of OAuth access tokens from different geographic regions, without full login events.

Log Sources

Mutable Elements

Field	Description
GeoIPDistanceThreshold	Minimum distance between token reuse events to trigger detection

AN0958

Container process uses mounted cloud credentials or token cache to authenticate without known orchestration.

Log Sources

Mutable Elements

Field	Description
ContainerLabel	Restrict to prod workloads or certain namespaces
CredentialPath	Path used to mount sensitive tokens (e.g., /.aws/credentials)

AN0959

Access token reuse to connect to SharePoint or Outlook APIs without interactive user context.

Log Sources

Mutable Elements

Field	Description
UserAgentCheck	Tune to detect access from CLI agents or scripts rather than interactive browsers

AN0960

Use of instance metadata tokens across instances or misuse of short-lived tokens issued for different roles.

Log Sources

Mutable Elements

Field	Description
TokenReuseWindow	Time window where token reuse is suspicious
RoleMismatchAlerting	Enable if tokens for RoleA are used in resources only RoleB should access

---