Detect Forged Kerberos Golden Tickets (T1558.001), Detection Strategy DET0144

Archived: 2026-04-05 13:59:03 UTC

AN0405

Detects forged Kerberos Golden Tickets by correlating anomalous Kerberos ticket lifetimes, unexpected encryption types (e.g., RC4 in modern domains), malformed fields in logon/logoff events, and TGS requests without preceding TGT requests. Also monitors for abnormal patterns of access associated with elevated privileges across multiple systems.

Log Sources

Mutable Elements

Field	Description
TicketLifetimeThreshold	Kerberos TGT ticket lifetime exceeding default domain duration; tunable to environment-specific policies.
AllowedEncryptionTypes	Valid encryption algorithms for Kerberos tickets; anomalies (e.g., RC4) may indicate forgery.
PrivilegedAccountPatterns	Baseline of privileged accounts expected to perform Kerberos operations; deviations indicate suspicious activity.
ProcessAllowlist	Expected processes interacting with lsass.exe; deviations may indicate credential dumping.