Detect Kerberos Ticket Theft or Forgery (T1558), Detection Strategy DET0522

Archived: 2026-04-05 17:05:31 UTC

AN1443

Detects anomalous Kerberos activity such as forged or stolen tickets by correlating malformed fields in logon events, RC4-encrypted TGTs, or TGS requests without corresponding TGT requests. Also detects suspicious processes accessing LSASS memory for ticket extraction.

Log Sources

Mutable Elements

Field	Description
TicketLifetimeThreshold	Threshold for Kerberos TGT lifetimes deviating from domain defaults.
EncryptionTypes	Monitor for downgraded encryption types (e.g., RC4) in Kerberos tickets.
ProcessAllowlist	List of expected processes accessing LSASS; deviations may be suspicious.

AN1444

Detects suspicious access to SSSD secrets database and Kerberos key material indicating ticket theft or replay attempts. Correlates anomalous file access with unusual Kerberos service ticket requests.

Log Sources

Mutable Elements

Field	Description
SecretsAccessThreshold	Alert threshold for frequency of access to Kerberos secrets files.
UnusualServiceAccounts	Baseline accounts normally performing Kerberos requests; anomalies flagged.

AN1445

Detects attempts to forge or replay Kerberos tickets by monitoring Unified Logs for anomalous kinit/klist activity and correlating unusual authentication sequences.

Log Sources

Mutable Elements

Field	Description
TicketRequestPatterns	Expected sequence of TGT followed by TGS requests; deviations may indicate forgery.
TicketLifetime	Expected ticket lifetimes; anomalies may indicate Golden or Silver Tickets.
