Detection Strategy for T1550.003 - Pass the Ticket (Windows), Detection Strategy DET0352

Archived: 2026-04-05 14:45:39 UTC

Analytics

- Windows

AN1000

Detects unauthorized Kerberos ticket injection by correlating service ticket (TGS - 4769) requests with absent corresponding account logons (4624) and prior Ticket Granting Ticket (TGT - 4768) activity. Highlights anomalous service ticket generation chains involving unexpected users, hosts, or times, and suspicious injection of tickets via mimikatz-like tooling into LSASS memory. Behavior also includes network lateral movement using Kerberos authentication absent expected interactive logon patterns.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Defines the correlation window between TGT request (4768) and TGS request (4769)
HostContextScope	Adjusts the host scoping for correlation of authentication chains and ticket injection
LSASSAccessAnomalyThreshold	Allows tuning of alerts for ticket injection attempts via LSASS memory access

---